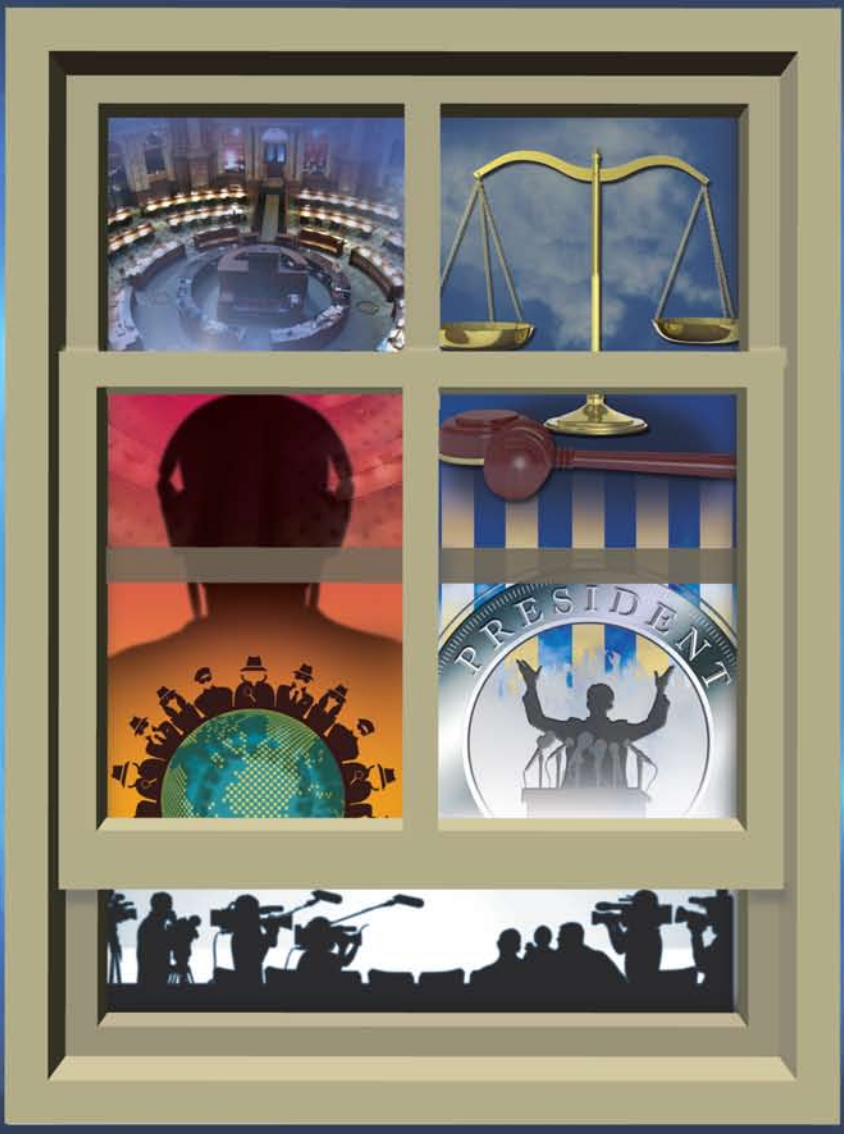
INTELLIGENCE MANAGEMENT
IN THE AMERICAS



Russell G. Swenson and Carolina Sancho Hirane
Editors

NATIONAL INTELLIGENCE UNIVERSITY

By focusing on the management of intelligence and gathering the analyses of highly authoritative writers, this work unveils nuances not normally found in previous publications. It dramatically reveals the incongruence of some existing intelligence organizations with democratic norms. The book will undoubtedly stimulate and refine the ongoing debate aimed at improving democracy in the region.

Luis Bitencourt, PhD
Professor and Dean of Academic Affairs at the Perry Center/National Defense University

This collection of essays offers the reader a unique yet comprehensive view of the historical, institutional trajectory of intelligence in most countries of Latin America and outlines the challenges facing political representatives and government officials who seek to improve the management of this government function under the rule of law in democratic societies. A key essay on the recent experience of the United States reorients the traditional conception of government intelligence and its management by highlighting an innovative field experiment in sociopolitical understanding in a foreign military advisory context. Overall, this is a useful book for professionals and students alike.

Thomaz Guedes da Costa, PhD
College of International Security Affairs, National Defense University, Washington, DC

In democracies, intelligence is now more necessary than ever precisely because it can help preserve an institutional framework for those who do not believe in a system where anyone may participate without constraint. In this context, however, there must be a reason for the government to gather information. Government intelligence was used for the wrong purposes in the dictatorial regimes that have afflicted the region. This led many democracies to have little interest in intelligence, an approach that is slowly changing. This book provides a well-documented assist to that restorative process. The range of contributions presented in this book makes us think about the next steps in the rehabilitation process, to include the adoption of international standardization in the uses and oversight of intelligence. In sum, this work helps us understand how states can address the intelligence function in the midst of complex, empirical realities.

Jaime Baeza Freer, PhD
Institute for Public Affairs, University of Chile

This book develops a good understanding of Latin American intelligence. In addition to its valuable comparative perspective, it sheds light in new areas, to include intelligence ethics, the role of intelligence communities, and prison intelligence. It also spells out the otherwise obscure relationship between public security and intelligence. As an anthology, it has special value in bringing together a select group of experts who, without redundancy, explore topics in a manner that will be of seminal value to practitioners and observers.

Antonio Diaz, PhD
University of Cadiz, Spain

Oversight of intelligence services in a democracy through judicial procedures is necessary to guarantee the performance of this state function in a manner that respects legitimate laws and the rights of citizens. Additionally, it is important for the services that oversight identify the limits of intelligence in terms of selection of targets and accountability for products offered and methods used, thereby reducing the use of intelligence for individual or partisan purposes. This book presents the work of 20 authors whose work covers the current status and the main challenges facing Latin American intelligence services as they contribute to the advance of democratic regimes.

Miguel Angel Esteban, PhD
University of Zaragoza, Spain

ISBN 978-1-932946-43-7
90000>
9 781932 946437

Intelligence Management in the Americas

Russell G. Swenson

and

Carolina Sancho Hirane
Editors

National Intelligence University
Washington, DC

June 2015

This anthology, *Intelligence Management in the Americas,* brings together the perspectives of 22 authors from across the Americas. They outline and assess the status and promise of intelligence oversight legislation and actions, and develop various arguments for preserving the best aspects of intelligence autonomy.

The goal of the NI Press is to publish high-quality, valuable, and timely books on topics of concern to the Intelligence Community and the U.S. government. Books published by the NI Press undergo peer review by senior officials in the U.S. government as well as outside experts.

How to order this book. Everyone may download a free electronic copy of this book from our website at *http://www.NI-U.edu*. U.S. government employees may request a complimentary copy of this book by contacting us at: press@NI-U.edu. The general public may purchase a copy from the Government Printing Office (GPO) at *http://bookstore.gpo.gov*.

Editor, NI Press
National Intelligence University
Washington, D.C. 20340-5100

ISBN 978-1-932946-43-7
Library of Congress Control Number 2012948533

EDITORS' PREFACE

In any country, intelligence institutions by definition form a first line of defense to protect citizens and their system of government. This book centers on strategic intelligence, a function whose purpose is to identify national-level threats, risks, and opportunities with respect to state security and public or citizen security.

Since the 1980s, responsibility for the management of a good part of state intelligence in the Americas has shifted from the hands of military and police establishments toward systems or communities with greater participation by civilians. Civilian intelligence entities specialize in addressing particular state needs and bring integrated attention to all the issues that might affect a country's national interests, including internal security. Adequate intelligence management now depends on the development of professional ethics, in addition to public intelligence laws and judicial oversight, to provide adequate supervision and control over intelligence activity.

This book addresses the present and future context for managing the intelligence function in the Western Hemisphere. This purpose obligates the authors to identify, highlight, and analyze the post-Cold War path of intelligence management, and to recognize successful experiments in its application. Authors consider the political, social, technological, and economic environments where this cognitive and operational discipline makes it mark.

This book builds on the observations and findings made in two earlier books. The first book focused on the development of professionalism during the democratic transition in the region, and the status of this aspect of intelligence at the beginning of the third millennium.[1] The next book examined the concept of national intelligence culture as a product of and spur to interaction between the "political class" and intelligence institutions in many countries of the region.[2] This third book continues the thematic approach as it examines intelligence management options that could be adopted by governments of the region. The authors and editors identify management challenges, examine best practices that may be exportable, and point out management issues yet to be addressed.

This publication features the work of authors who are experienced academics or government officials. Collectively, they aspire to understand and improve the management of intelligence across the region.

ACKNOWLEDGMENTS

The relationship between editors and authors is often mutually rewarding, and that collaborative ideal accurately describes the preparation of this particular project. Each of the authors has developed insights that reach well beyond their previous work to portray best practices, some already in place and others attainable and applicable to intelligence management at any scale. In addition to their appreciation of the authors' perseverance and patience, the editors would like to acknowledge the advice and assistance of manuscript reviewers (some of whose comments are presented in the book). In particular, we acknowledge Cathryn Thurston, NIU vice president for research, for her long-standing support of this project, and George Clifford, managing editor of the NI Press; Larry Hiponia, director of the NIU Center for International Engagement and his staff; Donna Wilson and Denise Hodges for their layout and design skills; and Andres Gonzalez Vargas, professor at the *Universidad Jorge Tadeo Lozano*, Bogota, Colombia, for artwork reproduced in the Alvaro Venegas Gonzalez essay. Finally, we are indebted to Julia Famularo and Andres de Castro Garcia for proofreading assistance. As always, any errors of commission or omission in this product are the responsibility of the editors.

Table of Contents

Table of Contents continued

Table of Contents continued

Table of Contents continued

List of Tables

List of Tables continued

List of Figures

Management of National Intelligence

Russell G. Swenson

"Think back, my dear; think back. We all become spies as children; that's the only way we know to make sense of the world."
—Amanda Cross, *An Imperfect Spy,* p. 224.

The essays in this book examine the democratic context of intelligence management across the Americas, where, increasingly, judicial and legislative oversight complement an ethical and professional commitment to professional practice. Intelligence contributes to public security, civilian and military planning, and even economic well-being. A civilian intelligence director from Mexico outlines this range of intelligence interests and responsibilities:

> Threats (present dangers) and risks (potential dangers) come not only from the so-called enduring themes of national security or from external sources, but also from the economic, social and political realm, and even the natural environment. Phenomena such as demographic trends, migration streams, social cohesion and inequalities, the informal economy, our delayed attention to the knowledge society and global warming, are all part of the new national security agenda.[3]

Intelligence can engage a country's civilian leaders and streamline the implementation of smart diplomatic, military, economic, and internally focused public security policies. The same Mexican intelligence official points out the unmistakable foresight that intelligence can bring to the public administration of national security issues:

> This way of looking at threats and risks lends itself to preventive thinking: how to disarm the risks associated with these themes, through a suitable system of indicators that would allow us, first, to identify and measure each potential danger to the components of national security (state, territory, population, constitutional order, democratic institutions, etc.), and second, to warn the various parts of the federal government, in a timely and appropriate fashion, to

> allow it to act opportunely. In this way, national security becomes a government-wide concern.[4]

The government-wide nature of national security, encouraged and sustained by intelligence, implies the existence of a broad range of state applications for this ancient government function, across numerous executive ministries or departments. At the national level *strategic* intelligence exists alongside *estimative* intelligence. In his essay on the foundations of state intelligence, an Ecuadorian observer explains the parallel concepts:

> Strategic intelligence addresses concrete and immediate issues, and it is proactive. Intelligence assessments are oriented toward prevention and they deal with long-term objectives. These two concepts are complementary and may be applied to any area of government concern, whether economic, political, social, financial or of any other sort.[5]

Beyond national strategic and estimative intelligence designed for presidents or prime ministers, ministerial or departmental intelligence also addresses truly strategic problems. As an example, we can point to the Operational Management Center of the System for the Protection of Amazonia (CENSIPAM).[6] As a permanent member of the Brazilian Intelligence System (SISBIN), CENSIPAM produces intelligence for SISBIN members across the Brazilian government. The often transnational risks and threats in the Amazon region present challenges to more than one Brazilian ministry. By a commonly employed definition, such multifaceted problems have strategic scope.[7] Another example comes from a unique description and analysis of intelligence decisionmaking within the "Threat Finance Cell" of Allied Forces in Iraq.[8] This cell hosted personnel from several U.S. Cabinet organizations, including the Armed Forces and the Treasury Department. Analysts in this unit made decisions of strategic consequence as a result of the capable guidance they provided to operational forces. These examples also illustrate the need for strategic intelligence in environments far removed from a national capital.

Even in the most globalized societies, the state intelligence apparatus focuses increasingly on the domestic environment. A country's internal environment exhibits social, psychological, and economic trends that, whether recognized

as such or not, influence and reflect security conditions in the rest of the world.

Security challenges with local and international effects include cybercrime; violent acts of terrorism; trafficking in drugs, arms, and human beings; contraband, money laundering, and piracy. The security tool most subject to citizen oversight, and well-suited to bringing knowledge to bear on these challenges, is government intelligence. Certainly, some states with global political and economic concerns, like the United States and China, devote resources at an astonishing scale to look outward and obtain knowledge and influence. Yet, government intelligence now largely examines the internal environment. This can be confirmed from the organizational diagrams of intelligence services worldwide, which often give administrative priority to internal order.[9]

An emphasis on individual, personal, or citizen security accompanies this internal orientation and makes careful management of the intelligence function necessary. The democratic rule of law, which has replaced the former "security state" associated with preserving the power of oligarchical or strongman rule in much of the region of interest, depends on identifying and ensuring the human rights of individuals. These developments suggest some pertinent questions. Has there been a reorientation of intelligence services as democratic institutions have regained a foothold in most countries? Has the combination of internal supervision and external oversight of intelligence, along with the occasional and highly public application of potentially influential international human-rights conventions, been enough to end the use of intelligence as a punitive instrument by executve branch officials against unwelcome challenges by individual citizens?

In carrying out the role that by definition includes advising elected officials at the highest levels, those in charge of the intelligence function bear the responsibility of cultivating and achieving a profound understanding of near- and mid-term issues and the accompanying opportunities for appropriate executive action. In the present work, authors will refer to some of these issues, but the aim of this book is not to catalog security threats or suggest how they may be resolved. Instead, it offers an exploration of the concepts, methods, and organization of intelligence in order to understand it as a sociopolitical and economic phenomenon subject to well-informed management efforts in the nation-states of the region.

Authors suggest that effective intelligence management will facilitate the exchange of information among the intelligence services of a government and among international counterparts. Political support that encourages such exchanges can help reduce, and perhaps prevent, the most dangerous acts of transnational criminal networks. Reaching this goal will depend not only on the professionalism of government bureaucrats, but also on the political class's ability to apply well-considered options to resolve key tensions in the intelligence management environment.

Four Echelons of Intelligence Management

The four sections of the book each address distinct intelligence management viewpoints easily distinguishable by their scale of responsibility. The first section explores the status of checks and balances among executive, legislative and judicial branches of government, as they apply intelligence oversight on behalf of a country's citizens. On a smaller institutional scale, the second section focuses on the management choices available to the executive branch itself. The third section moves on to the options available to intelligence services in managing the tension between privacy and security. Finally, individual intelligence services, with the opportunity to educate their personnel and integrate analytic communities of interest, come under review in the last section.

1. Intelligence Oversight in Democratic Context: Legislative, Judicial, and Executive Branch Checks and Balances

Key concepts: *Intelligence autonomy, national intelligence laws, judicial rules, and responsibility to citizens*

Any government that exerts concentrated power, whether considered authoritarian or not, can employ either their civilian or military intelligence services as "political police." Examples appear in all reaches of the hemisphere, highlighted by President Richard Nixon's attempted use of the Central Intelligence Agency to cover up his administration's involvement in the Watergate break-in[10] and the use of blackmail by Peruvian President Alberto Fujimori's intelligence chief to influence public officials.[11]

With the region's transition to democratic regimes in the late 20th century, one can begin to assess whether the management of various aspects of the national intelligence enterprise may also have become more democratic. Some

studies have addressed this question with respect to Argentina, Brazil, and Peru, and for the region's European relatives Portugal and Spain.[12]

Matei and Bruneau find that a serious reluctance on the part of policymakers (presidents and other senior political leaders) to get involved with intelligence reform issues leads to incomplete or hasty fixes to improve intelligence efficiency and ensure accountability. Policymaker reluctance to address comprehensive intelligence management stems from several factors. Two of the most important are a lack of strong public interest in administrative decisions and a siumultaneous unwillingness by policymakers to be associated with agencies historically tied to human rights violations. The politicians' preference for distancing themselves from intelligence management allows either new or legacy intelligence personnel greater latitude to press for the freedom of action and prerogatives they enjoyed in earlier authoritarian or laissez-faire bureaucratic arrangements. Furthermore, political leaders may at any time find it useful to collaborate with military intelligence organizations whose actions are not specifically made accountable by laws and regulations.[13]

Matei and Bruneau point out that incentives for reform of intelligence management can come from multiple quarters. One source stems from international pressure to conduct successful multilateral peace operations (Brazil's leadership of Haitian peacekeeping). Another arises from a clear awareness of serious threats (Brazil's attention to organized, violent crime). Still another comes from having insufficient intelligence to prevent high-profile crises (Argentina's being surprised by the Buenos Aires terrorist attacks of 1992 and 1994). Additionally, in 2004, the Peruvian media publicized various intelligence scandals (e.g., illegal wiretaps, selling of classified information by intelligence personnel), which led to executive and legislative-based restructuring of the national intelligence system, and to new intelligence personnel regulations. In Spain, as in Peru, legislative and judicial initiatives have followed media activism with respect to security and intelligence. In those countries, too, the executive branch through the Ministry of Defense has engaged in intelligence-related outreach activities with civil society. Matei and Bruneau conclude, however, that "[w]hile the perception of intelligence has admittedly changed within academia, it has yet to change among Spanish citizenry."[14]

In Portugal, the legislature has separated the production of national security, threat-related, preventive internal intelligence from police information. The

latter, in contrast, addresses criminal prevention and suppression through police action. In practice, this neat distinction does not account for overlapping realities.[15] It also does not allow for the use of new approaches to criminal intelligence. However, the division remains in place to aid legislative and judicial branch opportunities to distinguish national intelligence activities, which operate through secrecy and are to be subject to external oversight and control, from the more transparent criminal process involving police and courts. This divisive management strategy reduces the incentive for information sharing between the intelligence services and the police establishment, and encourages resource competition. Political wariness of intelligence secrecy, embedded in law, extends to disallowing the intelligence services from conducting surveillance or intercepting communications inside of Portugal, a prohibition likely to change in order to promote the international credibility of Portuguese intelligence in the eyes of foreign agencies who wish to collaborate on difficult cases involving transnational security and criminality. Portugal's overextension of controls on the actions of intelligence services calls for a more suitable management strategy where external controls do not interfere with the efficacy of intelligence services.

Another intelligence management issue with implications for public security involves the concept of intelligence ethics. An ethical sensibility by intelligence professionals, whereby thoughtful decisions must be made about who or what should be targeted, by what means, and under what circumstances, by definition appears where specific laws or regulations are not in place to determine what choices are to be made. The clearest path to defensible intelligence ethics lies in the answer to the question "How is the information being sought logically related to the principles (if any) spelled out in existing intelligence laws or regulations?"[16] If the principles are not supported, then the information should not be collected or sought. In the absence of relevant laws or regulations in any one country, practitioners may consult the array of less specific international human rights covenants, conventions, and treaties. At times, international standards may be effective moral and even legal substitutes for national guidelines.[17]

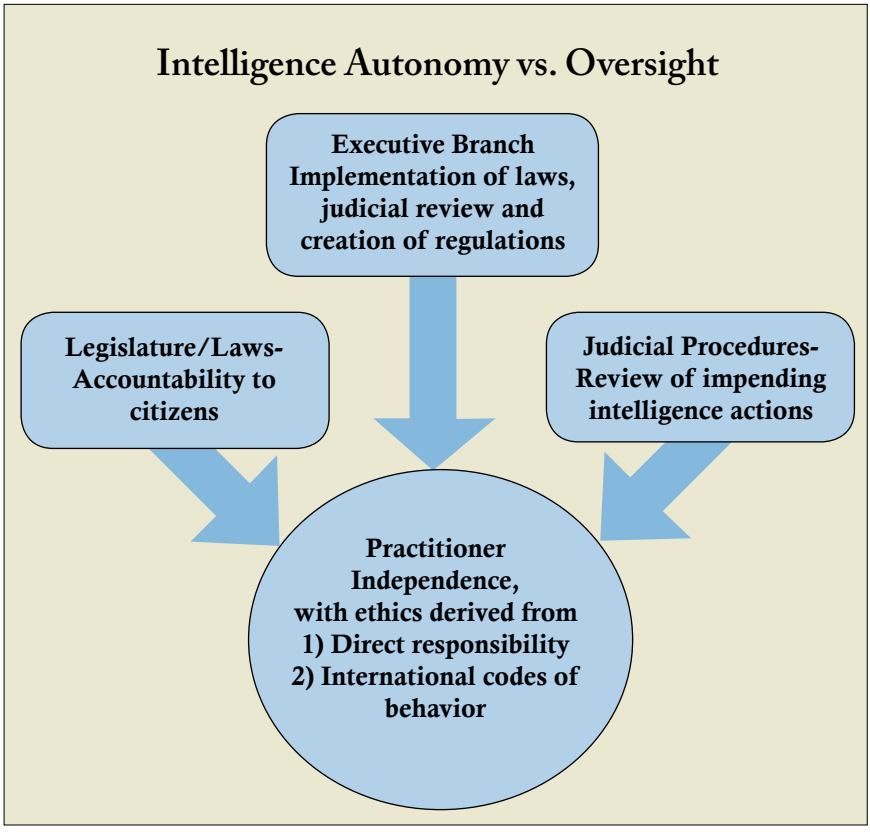


Figure 1
Source: Created by the author.

If a government fails to put in place and enforce appropriate laws and regulations, then the responsibility for deciding how to carry out duties that can easily infringe on individual privacy or even human rights, as defined in international codes of human behavior, falls to the intelligence practitioner. In this case, only the practitioner can be held accountable for unethical behavior. Therefore, under a rule-of-law regime, a powerful incentive exists for intelligence practitioners to support the enactment of intelligence laws and regulations. Ironically, an intelligence professional often accomplishes duties in a more robust manner when intelligence laws or regulations do exist.[18] Nonetheless, this zeal could be compromised if laws were to demand an extreme

degree of public transparency about a country's intelligence procedures to the point where analysts or collectors grow unwilling to risk taking action in the typically incomplete information and decision environment.

When intelligence practitioners do adopt an ethical approach to their work, it amounts to another justification for decisionmaking autonomy in the intelligence services. A good measure of autonomy allows an individual and an agency to build a reputation for sound, independent judgment. The expression of sound and independent judgment by an intelligence service improves its international reputation among professional counterparts who may seek help in tracking or neutralizing targets or gathering evidence for prosecuting a suspect. International intelligence collaboration reaches a deeper level of interpersonal exchange as countries with experience in countering internal threats, often overlooked in the past, offer new training cadres for others facing similar challenges.[19] The prestige of a country's intelligence services can become a public and popular measure of its own prestige and superficial attractiveness—whether positive or not—particularly if its intelligence or spy culture comes to be featured in films.[20]

Appropriate management can bring about trust in a country's intelligence services among all branches of government and the citizenry, as well as among international observers, and contribute to the ideal circumstance whereby improvements in the effectiveness and efficiency of intelligence activity does not detract from the individual or collective enjoyment of human rights. In brief, suitable intelligence management practices promote human rights. One observer has examined the competing arguments of pro-order and pro-civil rights coalitions in the region and suggests that intelligence and police internal affairs remain untouched areas of reform. He goes on to explain how reform efforts can be harnessed by advocacy networks to mobilize public opinion and establish greater accountability for intelligence and police functions. In turn, intelligence and police operations can be seen as complementing the protection, rather than the reduction, of individual human rights.[21]

The integrity of intelligence practitioners remains a concern, but legislative, judicial, and executive branch oversight and supervision mechanisms almost everywhere across the region help to guarantee and maintain that integrity. Naturally, these mechanisms do not work perfectly, just as the legal and ethical principles embodied in any law or regulation may not be enforced uniformly

and strictly. To maintain the integrity of the entire intelligence workforce, intelligence workers or professionals may occasionally need to release information on illegal practices to independent authors or news organizations so that public pressure can help steer the intelligence services back to approved practices.[22] The unauthorized or unintended release of sensitive information to print or electronic news media occurs frequently enough so that cautionary, pre-publication procedures can be established between government agencies and leading media enterprises to limit harm to intelligence capabilities or to public accountability.[23]

An insider may carry out the responsibility to maintain the integrity of intelligence services by publishing a fictionalized account of actual practices in an essay or a novel, or as the premise for a cinematic production.[24] This storytelling approach can accomplish the broader goal of educating the public and informing public officials with oversight and supervisory responsibilities about the motivations driving compliance and noncompliance with legal and ethical norms.

In the first section of this book, six contributions outline the institutional equities and the personal incentives at play in charting the tension between expressions of intelligence autonomy and external oversight. Some authors document the tortuous process of creating intelligence laws, which have become a common expression of external oversight, while others convey the central importance and viability of autonomy expressed through an ethical approach to intelligence work. The authors also address the noticeable constraints on intelligence actions brought on by judicial proceedings and by evidence of a continued negative public perception of this ever-present government function. A final commentary on the responsibility of the news media to shift attention from operational aspects of governmental intelligence to its legitimate strategic purposes eases the transition to the next section.

2. Intelligence Management within the Executive Branch of Government

Key concept: *Effectiveness of academics and other information entrepreneurs vs. professional civil and military services in informing democratic leaders*

Although a typical military commander expects trustworthy intelligence input into decisions, a civilian leader in a democracy learns to trust advisers who have helped him or her win the election. Without an opportunity to

build preelection trust with the new political leader, a country's intelligence services may be at a disadvantage in gaining this trust even after the election. This idea is reinforced by the research of a political scientist.[25] In her research, this investigator was able to obtain information from a survey instrument completed by government officials in the United States and the United Kingdom. Her results showed that in both countries, leaders used information from nongovernment sources as frequently as government information, even in making decisions related to the country's foreign policy. In contrast, an Israeli author contends that political leaders in democratic regimes tend to rely mainly on assessments from their intelligence services in making decisions with respect to international issues.[26] These studies may not apply to decisions on internal security, where leaders are sure to receive counseling from interested parties from inside and outside of government circles, and where intelligence advisers may lack the combination of objectivity and expertise to make their own voice heard.

Another more recent paper suggests that time-sensitive input from government intelligence specialists may not reach a senior policy official's desk because specialists simply lack the time to absorb the flood of open-source information related to the unique, isolated nuggets of information available directly from secret sources. Further, the author finds that the typical reliance on secret sources reduces the analyst's ability to "clarify issues such as climate change, energy security, global financial stability or food assurance."[27] At the same time, the author notes that senior political leaders may not even incorporate the occasional balanced *assessment* provided by government intelligence services into their decisionmaking process. Instead, they may "prefer the drama and clarity of a single-source report to the careful nuances" of any balanced assessments that might be available.[28]

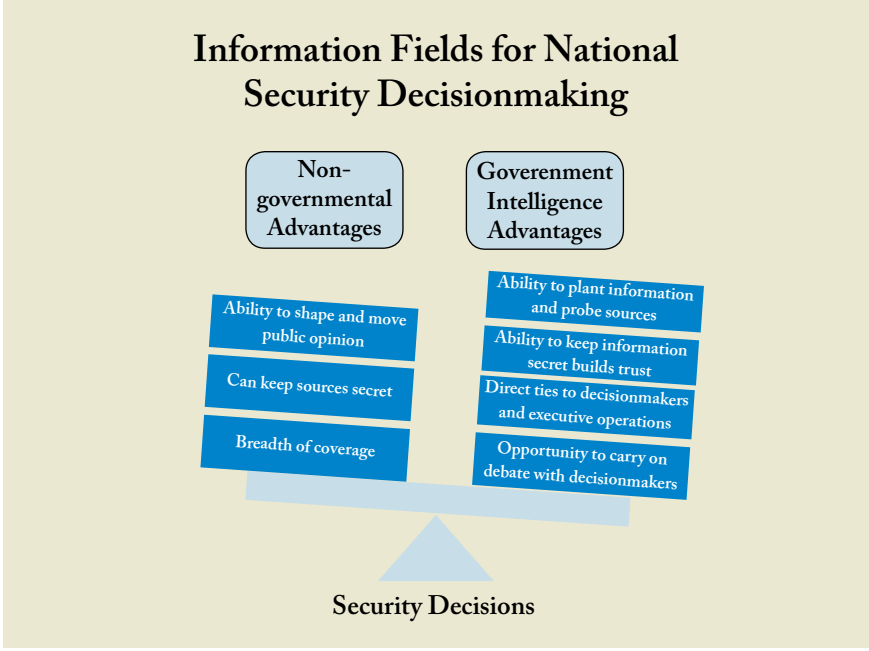


Figure 2
Source: Created by the author.

Whether the product of a formal body of intelligence professionals or of a diplomatic mission, strategic assessments made by government advisors likely have greater weight than the judgments, opinions, and recommendations—however well informed—of journalists, experts, or friends of policymakers. Government officials have generally direct access to those who make decisions and establish policy. They also have access to the forces, whether civilian, military, or mixed, that carry out the chosen policy.[29] Access to secret information sources gives government officials another advantage. To the degree that they can maintain secrecy, officials will gain the confidence of a decisionmaker. Additionally, by virtue of the capabilities of any country's intelligence services, its functionaries can expect to have information collected under covert or clandestine conditions to confirm, or preferably refute, a working hypothesis. This capability includes the opportunity to plant false information, leading the intelligence target to reveal plans and intentions. Finally, decisionmakers expect that government officials will not leak sensitive information, not a difficult

guarantee for an intelligence professional to fulfill, as trustworthiness remains a central value of intelligence culture.

An enduring theme of intelligence management involves the nature of the relationship between the highest elected officials of a particular government and the intelligence personnel who provide assessments and judgments on key issues. Practitioners often ask themselves whether to develop empathy with the official they inform or advise. Should they empathize with that official's vision of the world and of the issue at hand? Or should they maintain a psychological and substantive distance from the official? By maintaining that distance, an intelligence professional may make himself or herself less likely to collude with the public official.

Some observers and intelligence practitioners recommend against maintaining a psychological distance from the public official charged with deciding a policy or action. Robert Gates, later Director of the Central Intelligence Agency and Secretary of Defense, wrote about his experiences as National Security Advisor in the administration of President George H. W. Bush. He discovered that the tendency for Intelligence Community personnel to hold White House officials at a distance did not accomplish positive results.[30] Intelligence officials often consider "working too closely with" high-level decisionmakers (that is, taking into account their policy objectives) an invitation to politicization, where either side adjusts assessments or selects information to justify already-chosen policies. Yet, Richard Betts finds that working closely with senior political officials holds benefits so long as intelligence "does not misrepresent but packages information in a way that prevents it from being shunted aside as irrelevant."[31] Another author calls for officials on both sides to go beyond thinking of intelligence as policy-neutral "information support," and instead acknowledge its direct role in providing "decision advantage": Intelligence yields a decision advantage through responsible, evidence-based rhetorical persuasiveness.[32]

Two current U.S. government officials explain why policy-oriented intelligence should not be discounted. Kerbel and Olcott recognize the idea that high-level officials will use all sources of information, many of them from outside the government. In their experience, responsible senior officials often welcome personally presented intelligence judgments that teeter on the brink of recommending a policy. High-level officials appear especially eager to learn

the intelligence professional's view of the likely results of the recommended course of action.[33] This point of view runs squarely against the tradition in the U.S. Intelligence Community, originally promoted by Sherman Kent, of maintaining intellectual distance between a "pure" intelligence judgment and the less-pure political world. The approach suggested by Kerbel and Olcott, though not yet widely employed, could bring about a fundamental change in the way intelligence personnel approach the principal decisionmaking officials of the United States.[34] The U.S. Intelligence Community already employs "adversarial briefing" to improve communication between an intelligence functionary and the responsible official. It consists of a series of meetings attended by the responsible official and two intelligence personnel who take contrasting positions on an issue of interest in a debate format. This technique gives intelligence personnel another decisive advantage over competing information sources in terms of their potential influence on security-related policy decisions or actions.

Economic threats and opportunities have become a central intelligence concern because no country can escape their international expression.[35] Globalization means that foreign influence has internal manifestations. The Financial Intelligence Units of the Egmont Group, an international nongovernment entity, already confront money laundering activities in several countries of the region.[36] The spread of financial crimes and economic threats of a more general nature suggests the further development of economic intelligence capabilities.

A French author asserts that a national government serves as a country's ultimate guardian against economic threats, even when it holds membership in a formal, multinational economic alliance.[37] A provocative book pinpoints a series of historical events that created the fundamental shape of today's world economic relationships.[38] Can government functionaries responsible for economic intelligence assessments identify "future history" trends and events of transcendental importance at the national level? Or will decisionmakers rely on assessments by financial industry experts whose long-term loyalty to government interests may be doubtful? Recognized experts can work in, or even create, offices or agencies for economic intelligence. If they are willing to engage in economic intelligence analysis over many years, they will have given proof of their loyalty to the well-being of the state and its citizens. A sound

management approach would challenge analysts to understand economic affairs through large-scale exploitation of open-source information.

The absence in recent years of wholesale dismissals of seasoned intelligence functionaries across the region serves as a positive indicator of wise management. Such abrupt dismissals have taken place in the United States, Argentina, Mexico, Peru, and Colombia.[39] The loss of individual experience by definition reduces institutional knowledge. In the end, management of intelligence services through careful executive branch decisions can ensure a comprehensive, corporate understanding of security issues and the means to address them through accountable government resources.

The five essays in the second section of this book explore some of the intelligence management opportunities that await executive branch officials in the Americas. Each of the authors points out how intelligence practitioners can take advantage of existing or potentially innovative communication strategies to help national leaders expand national and citizen security.

3. Intelligence Community Management of Privacy and Security Issues

Key concept: *Use of police intelligence vs. national intelligence institutions to address internal security issues*

The same motivations and trends that have resulted in an increasing range of government intelligence offices and agencies can create long-lasting obstacles to the integration of intelligence communities. With its new Department of Homeland Security, the United States has expanded but not yet integrated its intelligence capabilities. Outside of the national level, the cities of New York, Dallas, and Los Angeles have developed notable police intelligence capabilities. The adoption of intelligence methods by police forces has become a tool for crime prevention. The police focus on crime prevention is a function of criminal activity becoming less random; that is, it has become a more organized phenomenon. The organized nature of criminal groups implies that their activities are planned, a development that gives an opening for the use of preventive methods by the police. This preventive approach toward threats is similar to that of the national government, but notably without any collaboration with national intelligence agencies.[40] In an environment of abundant resources, instead of integrating their efforts across a community, intelligence

organizations proceed independently to collect information relevant to local needs in a bureaucratic and geographic sense.

In combination with the expansion of government intelligence agencies in the United States, a perceived "wall" has inhibited the exchange of information and assessments between the world of police intelligence and national security intelligence.[41] This wall has never existed as a formal, legal barrier to the exchange of information or intelligence.[42] It was, and remains, an artifact of the political nature of the intelligence function. From the beginning of the "war on terrorism," an error of omission, as in the failure to prevent the attacks of 9/11, has prompted intelligence leaders and outside observers alike to blame the "system," rather than assigning blame to the errors of individuals or of particular intelligence agencies. If a *system* problem does exist, then adjustments to the system may improve performance. For example, given the separation between police security and national security, what arrangements would promote the exchange of intelligence information between the national security elements and local police? Are informal exchanges among intelligence practitioners enough to overcome the divisive elements of the system?

A diplomatic police official provides an initial, positive reply to this question. [43] He explains that the police forces of countries worldwide now often agree to share local information with their foreign counterparts, particularly if that information has value for prosecutions. So much cooperation exists, in certain cases, between U.S. diplomatic police and their foreign counterparts that local officials can decide to share information without obtaining prior approval from their own national officials.[44] This reality also reflects the political distance typically maintained between local police and national authorities in any country.

Yet what do we know about the occurrence and consequences of this type of information sharing within a country? Given that informal exchanges do occur, how can we develop and manage an information structure and practices to take greater institutional advantage of informal, personal relationships among intelligence personnel? That is, can we build institutions to advance internal and external national interests through the informal exchange of security information, to include its synthesis into intelligence?

One answer to the last question appears in hybrid forces that take a military-style approach to internal security, but that at the same time have police powers. These hybrid forces also emphasize safeguarding citizen rights through legal police procedures. Two examples of this institutional innovation are the U.S. Coast Guard and the Argentine *Gendarmeria Nacional*.[45] However, local police operate principally on the basis of human intelligence, rather than using the more technical collection disciplines like signals intelligence or imagery intelligence common at the national level. Even though there may be a need for national information to combat transnational criminal activity in one locality, national intelligence organizations often choose not to share information with local police. This is because community police typically do not reciprocate by sharing information about local issues, even when the information may also be of national concern.[46]

A continuous and intrusive national police operation would be required to gather, coordinate, and act on information collected from across an entire country. Such a pervasive presence would remind residents of the reviled "security state" approach taken by earlier, authoritarian governments. In democratic societies, "national security" is a concept remote from daily life and also something over which citizens seem to have little or no power.[47] In recently authoritarian countries, the concept will have negative associations. Could a marked increase in intelligence resources for provincial and city police, within the context of a decentralized policing and information-gathering paradigm, build capabilities to address national or transnational criminality, without reminding citizens of the political police of the "security state"?

Figure 3 illustrates the comparative advantages for citizen security offered by national police or intelligence services that become involved in ensuring internal security. Each of the five points of comparison is presented in the same order in each column. As a comment on the last of the five points, national involvement in local affairs is often unwelcome. However, visible adherence to international norms, required of national security forces as they attempt to gain or maintain a positive public perception in the international environment, may offset any corruption found in local citizen security institutions. A positive international image can increase a country's opportunities for securing international security resources.

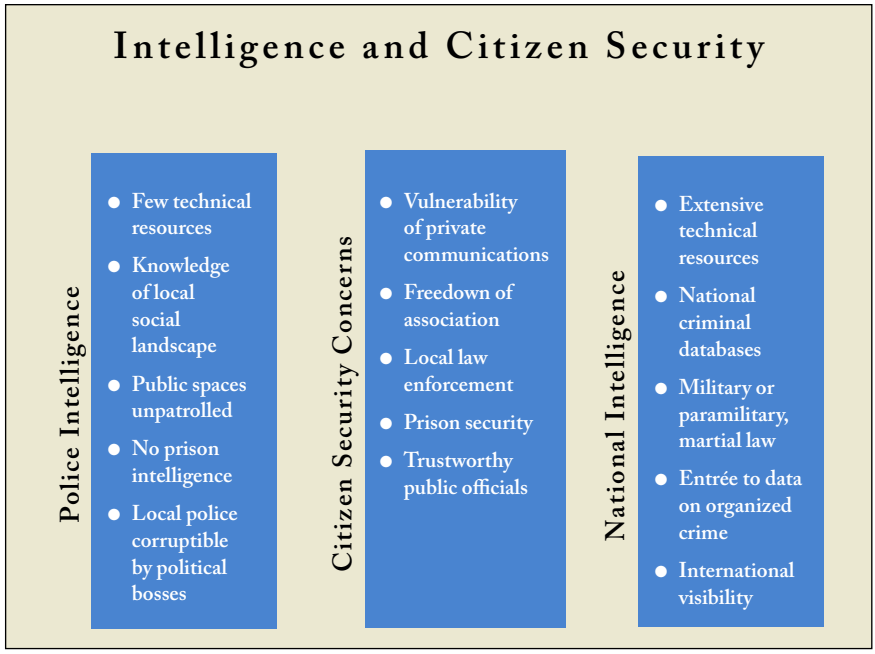


Figure 3
Source: Created by the author.

Community policing, increasingly known to practitioners as intelligence-led policing, may offer a reasonable alternative to a centralized, national approach to developing intelligence information for internal security.

> Today, police reform advocates throughout Latin America seek to respond to demands for public safety by promoting community policing models. Although it is ill suited to carry[iing] out the organizational heavy lifting that fighting transnational criminal organizations requires, such advocates argue that community policing helps to demilitarize, democratize, and decentralize law enforcement institutions, putting an operational emphasis on agents in-the-field judgment and greater control over the use of force.[48]

The development of preventative intelligence also implies that it will be used for some purpose. Local police could lose the trust of the communities they serve if their information were to be added to a national criminal database, rather than being used for the clear benefit of locals. This possibility may help explain why national databases, such as Mexico's *Plataforma Mexico* and Brazil's *Sistema Nacional de Informações de Justiça e de Segurança Pública* (INFOSEG), have been slow to incorporate information from local police or other security organizations. Nonetheless, as local criminality blends with national- or international-scale criminal enterprise, opportunities for provincial or city intelligence to become institutionalized also increase. An ilustrative case comes from Mexico.

The northeast Mexican state of Nuevo Leon recently adopted a law specifically penalizing the activity of "lookouts" used by drug-trafficking organizations to spy on police and military activity. The law may threaten the freedom of action of the traffickers.[49] The federal structure of the Mexican government offers each state the opportunity to develop similar laws to reduce the incidence of impunity. The Nuevo Leon measure targets local "employees" of trafficking organizations, and signals a notable community investment in the rule of law. The degree to which this law and others like it are enforced will determine whether the foundational rule-of-law concept applies to daily community life.

Community policing, including intelligence-led policing, experiences local political influence, or "corruption."[50] A leading expert on community policing in Latin America explains the process:

> Citizen-based security initiatives are often hobbled by the citizens themselves. Neighborhood councils and patrols become co-opted by neighborhood commissioners, by drug traffickers, or by program directors who channel funds to their friends.… Most communities are deficient in the cohesion, finances, and experience needed to form durable groups that can consistently identify the causes of insecurity—much less break down the fear, distrust, and violence that characterize their relationships with the police. As economic trends continue filling poor urban areas with

> newcomers, even established neighborhoods have difficulty maintaining community organizations, in turn limiting the knowledge and information that reach the police.[51]

The same author asserts that in Mexico City, fully 70 percent of police protect businesses, rather than acting on behalf of local government authorities and the public at large by patrolling a "beat" in public spaces.[52] Similarly, another long-time observer of regional criminal justice tendencies notes that in Argentina, unpatrolled public spaces outside of "gated communities" continue to grow in size and level of violence.[53] To the degree that these findings represent the geography of policing in the region, the lack of police circulation in public spaces offers little opportunity and even less incentive for local police to gather information useful in preventing or prosecuting crimes. These observations, together with political co-optation of police activities in individual cities and provinces, reduces community willingness to provide information to the police. Unless legislative and judicial activism becomes more widespread and effective, local police should not be expected to contribute meaningfully to the perceived or actual improvement of internal or citizen security.

One would expect the largest cities of the region to have the resources and public visibility to promote an effective, if not efficient, police-based intelligence enterprise. However, outside of the intelligence force of New York City,[54] with its international reach, and Rio de Janeiro's police intelligence force popularized in the film series *Tropa de Elite*, there is little evidence that urban police forces have reached the level of intelligence professionalism or integrity expected of national or federal police forces. New York City likely has the most expansive police intelligence establishment of any city in the hemisphere. Yet, critics point to its limited capability for analysis, and in contrast with national intelligence agencies, it has only *ad hoc* guidelines on what information to collect.[55] Unrestrained information collection against Muslims by New York City's Police Intelligence Division has been widely publicized and strongly criticized by human rights organizations as well as by the Federal Bureau of Investigation.[56] The FBI's domestic intelligence operations, in contrast to those of the New York City Police, must observe strict civil liberties guidelines.[57]

Several options exist for the improvement of intelligence management as it affects citizen or public security. "Social intelligence" capabilities at the national level can be combined with the detailed knowledge of local community political officials or community police. This approach is explored in essays on Mexico and Guatemala in this third section of the book. Another essay addresses the need for generating intelligence in a country's prison system, where one might expect to gain useful perspectives on the operating details of organized criminal enterprises. A combination of national intelligence information resources and local familiarity with the hallmarks of criminal franchises could lead to a more effective form of exploiting information-collection opportunities in penal institutions. Finally, one essay explores the pervasive influence of military intelligence conventions in Brazil, a reminder of the obstacles to achieving integration of intelligence institutions.

4. Managing Intelligence Integration: A Challenge for Intelligence Services

Key concept: *Information sharing across government, together with public transparency, allows for the integration of the "deep knowledge"of intelligence professionals with societal values. This ideal is promoted by developing robust professional intelligence education, promoting public/private collaboration in cyberspace, and engaging in field experiments of information sharing among advisory personnel in a multinational international engagement environment.*

Intelligence integration typically refers to the collaboration expected among the disparate agencies, offices, and organizations that make up a country's intelligence system or community. However, this restrictive vision masks a larger view of integration. The larger concept of intelligence integration envisions ways to combine intelligence information with "open" information to bring about improved security decisions and actions across a society. The formation and eventual maturation of this approach depend on initiatives taken by the intelligence services themselves, albeit with the support of politicial authorities. Traditional intelligence services severely restrict access to and analysis of classified information to a select group of individuals who voluntarily subject themselves to monitoring for trustworthiness and compliance with confidentiality norms. Therefore, only those individuals and their respective organizations can monitor the flow of information and make the decision to share it with other agencies, so long as laws and regulations have provided them the bureaucratic freedom to do so. Legislative and executive

attention to the "responsibility to share" information across government entities and beyond typically appears only after egregious failures by intelligence entities to detect and prevent politically powerful events.[58]

The three essays in this section illustrate how an intelligence system or community, through its own management decisions, can address a society's security needs. It can do so by going beyond the traditional approach intelligence agencies have taken, moving away from a restrictive view of national security and defense and toward promoting the well-being of a society.

National intelligence services often have an institution—a civilian, graduate-level school—that is unique in allowing practitioners to step back from their routine work to contemplate the place of intelligence in their society and how to improve its performance. It appears that intelligence education institutions can influence, through their curricula and the skills of the faculty, other, larger intelligence institutions in the armed forces and the civilian intelligence services of a state. That is, intelligence schools do not simply mirror the practical experiences of students and their home organizations. Instead, at their best they imagine and illuminate the social and technical phenomena of national intelligence from a broad and even theoretical perspective, always with an eye to carrying out experimental and applied research.

National intelligence schools, either civilian or military, figure prominently in the intelligence history of some countries.[59] We also know that intelligence practitioners from friendly countries attend classes or participate fully in the programs of some intelligence schools.[60] However, we do not know the nature and extent of personal and professional interaction in the intelligence schools that regularly host foreign students. It may be that such schools are fostering a broadly based understanding of how best to manage this government function across the entire region. An essay on intelligence education in this section points out that some national intelligence schools enroll students from a cross-section of society, including individuals with legal, commercial and various academic backgrounds.

Cybersecurity is a natural concern of intelligence services, as the security and integrity of economic activity as well as defense capabilities now depend on the invulnerability of digital communications. The institutional framework for this relatively new sphere of intelligence activity is not yet well established

anywhere. The responsibility to identify and even prevent attacks offers fertile ground for integrating private-sector with public-sector information capabilities, as well as civilian and military intelligence competencies.

Although intelligence involvement in cybersecurity may worry individual citizens, they face an even more pervasive threat of invasive penetration by private-sector individuals and institutions. Where privacy is most valued and expected as a human right, namely in private and familial communications, vulnerability to loss of privacy is greatest. Although one might blame government eavesdropping for the loss of privacy in personal communications, clearly Facebook, Google, and other social media have the greatest opportunity and perhaps the greatest incentive to take advantage of personal information for their own benefit. At the same time, less-pervasive government interception and use of private communications is seen as a greater threat because of the government's near-monopoly over legal coercion.[61] The continued use of Facebook, Google and similar services by millions of users suggests that the benefits obtained in the form of easier personal information-gathering and communication still outweigh concerns over those enterprises' exploitation of the user's private worlds. Yet, any invasion of privacy by a country's intelligence services is challenged as unjustified, even though the work responds to public laws and the legitimate needs of individual political leaders. The essay on cybersecurity in this section suggests that despite collusion between a country's intelligence services and its communications enterprises, the ethical and legal integrity of intelligence officials allows them to justify the government's "nonprofit" work on behalf of public security.

In some contexts, practitioners cannot identify their work as "intelligence." An example comes with the implementation of the "Smart Power" approach to U.S. foreign policy. Smart Power enlists non-military sources of influence to achieve foreign policy objectives. In the example developed for this section, collaborative development of democratic institutions in a challenging advising environment has fostered a new approach to information handling outside of the formal reach of intelligence activity. This new type of information organization and its corresponding operating procedures constitute an alternative to traditional, threat-oriented intelligence.

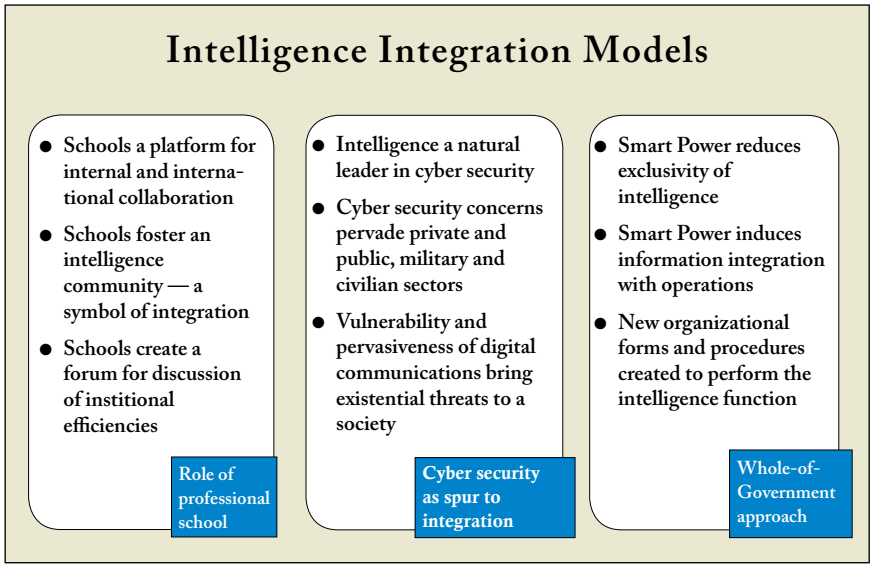


Figure 4
Source: Created by the author.

Intelligence services, like any bureaucratic organization, have an interest in self-preservation and growth. To achieve those ends, they need to demonstrate their value on a daily basis. Not only that, but they also need to demonstrate the superiority of their products over those of potential competitors in anticipating and meeting the needs of official users of information and assessments. Competitors include news media, academic professionals, public and private research centers, and any group with ready access to pertinent information that can be verified. Uniquely, intelligence services are obligated to demonstrate their readiness to understand and expertly advise on how to engage emerging threats and opportunities.

To remain relevant and dependable, all intelligence services face the challenge of identifying and hiring already well-educated and trustworthy prospective employees, providing stable career paths through technical training and the development of deep target knowledge, and then continuously educating their workforce through world-class professional development programs.

Both postgraduate intelligence education and an intelligence focus on public cybersecurity have the potential to integrate the efforts of government and nongovernment security institutions and their personnel. At the same time, in the contemporary military environment where individual officers from advanced countries are expected to invent a credible process for advising local, high-level national officials on the design and implementation of accountable national security institutions, one finds a requirement for rapid innovation and integration of information gathering in a bilateral or multilateral environment.

The function of information gathering and handling cannot always be labeled "intelligence" because of local and international sensitivities and even legal restrictions on the activity. However, personal interactions in the context of gaining and processing useful information for national security purposes serve the same purposes as national or strategic intelligence. Thus, field-based advisor teams create and manage an integrated approach to multilateral information handling and analysis, which may also be called multilateral intelligence.

Layout of the book

Each of the four levels of intelligence management is addressed by essays in this collective work. To introduce each section, well-qualified observers and participants from across the Americas bring their expertise to bear as they place each set of essays into academic and professional perspective.

Section One

Intelligence Oversight in a Democratic Context: Legislative, Ethical, and Legal Dimensions

Commentary on Section One

Marco Cepik

The essays that make up the first part of this book address the legitimacy of national intelligence systems, and in particular explore the legal apparatus that regulates, controls and oversees intelligence. The essays also examine the philosophical context of intelligence, as it contributes to the development of a professional ethos within government services.

Andres Gomez de la Torre Rotta and Arturo Medrano Carmona examine how the Peruvian legal framework has contributed to the evolution and institutional design of that country's intelligence system. They also give brief attention to other national experiences in the region. The essay explores legislative history from an empirical perspective. Among the most interesting are Law 29915/2012 and Legislative Decree 1141/2012, aimed at strengthening the connections between security, defense, and intelligence, as well as the proper role of the *Dirección Nacional de Inteligencia* (DINI).

Joanisval Brito Goncalves expertly addresses the variety of controls that can be applied to intelligence in Brazil and other countries, particularly Canada. The author's opinion of the Brazilian Law on Access to Government Information (Law 12527 of 2011) reflects the concern tbat government officials have about this law as a matter of principle. However, that opinion overlooks the problemlatic lack of a fundamental, empirically and theoretically informed debate about governmental secrecy and the public right to information like the conversation that has taken place over the past two decades in the United States.

Carlos Maldonado Prieto examines ethics in intelligence through an appropriate analytic framework. His opinions and perceptions are informed by close observation of Latin America and Eastern Europe institutional developments. This author or others could dig deeper into the relationship between intelligence and international law, only briefly addressed in the present essay. This relationship underlies any discussion of a potentially universal set of ethical norms for intelligence. In particular, the question of political assassinations could be framed as part of the relationship between those undertaking covert actions and the governmental offices responsible for intelligence oversight.

The author wisely highlights the ethical significance of treating intelligence as a public service in the contemporary world.

In "Human Rights and Intelligence Ethics: Cases from Cinema," Moira Nakousi Salas and Daniel Soto Muñoz explore the problem of carrying out intelligence activities within a democracy. In a democracy, the intelligence requirement to prevent or repress a threat conflicts with the social costs of restricting individual rights and freedom. As the authors point out, the film industry has explored this dilemma in some well-known works. Drawing on three of those works, they stress the need to ensure that methods of intelligence and counterintelligence adhere to judicial and ethical frameworks. The authors explore three scenarios: the violation of the right to privacy by East German political police in *The Lives of Others* (*Das Leben der Anderen*) (2006); the impunity of a common criminal employed by a security agency during military rule in the Argentine film *The Secret in Their Eyes* (*El secreto de sus ojos*) (2009); and especially, the examination of whether a terrorism suspect should be tortured in the 2009 film *Unthinkable*.

Together, the four chapters of this section represent a thoughtful approach to the legal, ethical, and political aspects of intelligence management in the Americas.

Marco Cepik serves as associate professor at the Federal University of Rio Grande do Sul (UFRGS, Brazil, *http://lattes.cnpq.br/3923697331385475*). He is also director of the Center for International Government Studies (CEGOV, *www.cegov.ufrgs.br*). **Contact:** *marco.cepik@ufrgs.br*.

Intelligence Laws in Peru and Latin America—Historical, Legal, and Institutional Evolution

Andres Gomez de la Torre Rotta
with
Arturo Medrano Carmona

"The third article [by Luis Iberico] highlights the communitarian promise of a society that takes its destiny into its own hands by reinventing the State and its services."[62]

—Fernando Cocho Perez

Prologue

As of 27 January 2012, the Peruvian National Intelligence Service (SIN) would have been in place for 52 years as the country's principal, civilian, high-level political/strategic organization. However, on 14 September 2000, it was dismantled because it had performed or subcontracted intelligence services for partisan political ends.

Introduction

This essay examines the origins and evolution of Peru's successive national intelligence laws and their shortcomings. It also highlights parallel legal developments in Panama, Colombia, Ecuador, Uruguay, Venezuela, and Bolivia, as these countries move toward the oversight and control typical of a democratic intelligence framework. This typical framework features three types of external control: congressional or legislative,[63] judicial,[64] and economic or financial.[65]

The essay asks where the region stands with respect to the continuous tension among executive, legislative and judicial branches where intelligence services operate under the rule of law. Centralization tendencies provide greater autonomy to the executive branch and its intelligence organizations, while decentralization brings greater external oversight from the legislative and judicial branches.

Diego Navarro Bonilla reminds us that "intelligence has historically been associated with the idea of secrecy."[66] Despite that secrecy, this essay explores how this government function can be improved within a democratic context by examining issues ranging from the academic background of intelligence professionals to the nature of democratic control mechanisms.

Origins of Government Intelligence in Peru

The establishment of Peruvian government intelligence began with military intelligence units in the armed forces. By the end of the 1950s, army generals had created an intelligence service and an intelligence school whose graduates dominated the development of Peruvian intelligence through the succeeding decades. Given their affinity for the French military, the army absorbed, among other ideas, French concepts of "security, development, and pacification." The French later imparted a counterinsurgency mindset as a result of their experiences in the Algerian War of Independence.[67]

As part of its decade-long institutional modernization, the Peruvian Army established a strategic intelligence organization, the nominally civilian National Intelligence Service (SIN). An executive order (un-numbered) created the SIN on 27 January 1960. Another, complementary executive order on 30 September 1960 set forth additional guidelines for the institutionalization of the SIN within the governmental apparatus, identifying its makeup and authorities. One part of this executive order articulated the relationship of the SIN to other government ministries.[68] The use of executive orders to establish and regulate intelligence activities reflects Peruvian legal practice.[69] As Victor Garcia Toma states, executive orders "are concerned with the more general aspects of how ministerial and inter-ministerial activity is regulated at the national level. They establish and oversee the organization and functioning of national public service institutions, together with the activities of these entities."[70] Garcia Toma suggests that national intelligence constitutes a "public service," and its inclusion in the name of the "National Intelligence Service" dates from this executive order.

One can view the Peruvian National Intelligence Service as a product of the Cold War, with its focus on fighting communism and counterinsurgency. Cold War nomenclature characterized intelligence institutions across the region: the SIDE and SFICI in Argentina and Brazil, respectively (1946); the

DFS of Mexico (1947); and the SIC-DAS of Colombia (1953). Later, Venezuela would follow with its DISIP (1969), supported strongly by the United States and its own intelligence agencies during the democratic government of President Rafael Caldera (COPEI).[71]

None of the executive orders from 1960 anticipated the emergence of restrictions on government intelligence. However, it should be pointed out that these mandates were only initial efforts to deal with intelligence institutions and their function. They appeared in the wake of the Chinese (1949) and the Cuban (1959) revolutions, and as irregular, insurgent, and revolutionary aspects of internal conflict were growing in the region. The executive order of 27 January 1960 refers to that environment:

> The complexity of the problem that our National Defense now faces makes necessary the establishment of special organizations so as to better accomplish the obligations that the Constitution and our laws place on the President of the Republic.

The order established that, as a subordinate entity within government, intelligence produces a product for a privileged consumer or decisionmaker. Actions by the decisionmaker, in turn, take place within boundaries established by the constitution and relevant laws.

Evolutionary Developments in Peruvian Intelligence Legislation: 1960–1970

Leaders began to employ the Peruvian National Intelligence Service for political purposes in the 1960s, during the democratic regime of the Popular Action President Fernando Belaunde. The SIN worked with the Ministry of Government and Police in 1965 to impound Marxist books and pamphlets. This was done to combat the influence of pro-Castro guerrillas who were operating in Peruvian territory under an insurrection model exported from Cuba. Of course, Army intelligence also focused on the insurrection. In fact, the predominant role of military intelligence, especially within the army and marines, manifested itself in a military coup d'etat on 3 October 1968. Army intelligence drove the coup, with no participation by the SIN.

Two top officials of the SIN reacted to the coup very differently. Its leader, General Carlos Linares Molfino, resigned his position because of his close ties with the constitutional President Fernando Belaunde. His deputy, Colonel Eduardo Segura Gutierrez, yielded to the military putsch and later became the head of the SIN.

On 25 March 1969, the Revolutionary Government of the Armed Forces, headed by General Juan Velasco, issued Organic Law 17532 of the President of the Republic. Its article 2 subordinated the SIN directly to the president of the republic.

Finally, Law 19351, which amended the executive order of 30 September 1960, explained how members of the National Intelligence System (SINA) should coordinate with each other. However, this law failed to address the issues of accountability, democratic controls, supervision, or oversight of intelligence.

Laws promulgated in the 1960s remained in effect through subsequent political regimes. An action by the Revolutionary Government of the Armed Forces (1968–1980) promoted this continuity. Law 19351 of 1972 put in place a legal "theory of continuity," whereby laws enacted during the military regime would not expire when Peru returned to democracy. This law remained in effect well beyond the return to democracy in 1980. Legislative Decree 270, article 29 finally superseded this law on 10 February 1984.

The War against Terrorism: 1980–1990

In 1980, the Peruvian Communist Party-Sendero Luminoso (PCP-SL) started a revolutionary, unconventional war against the Peruvian state. The PCP-SL employed various criminal methods and prompted a thorough review of counterinsurgency plans. The counterinsurgency plans of the National Intelligence System were among those reviewed.

Law 23720 of 1983 gave the executive branch the power to make decisions with respect to intelligence. The Peruvian Congress thus exerted no influence over intelligence management. The executive branch took action to improve the structure and aims of national intelligence with decrees 270 and 271. The first refined the National Intelligence System (SINA), and the second addressed the SIN itself. These decrees appeared during the bloody

and no-holds-barred insurgency, at a time when the SIN was led by a Navy official. The Senior Intelligence Council, created by decree in 1972, pushed for the adoption of the measures as a way to build a positive association between intelligence and democracy.

Testimony from later SIN leaders reveal unsuccessful efforts in 1984 to reform and improve intelligence laws. Gustavo Gorriti Ellenboghen, a Peruvian journalist, writer, and opinion leader, devotes an entire chapter of his book on the *Sendero Luminoso*[72] to the country's intelligence services in the 1980s. The chapter, "Conclave of the Blind: The Intelligence War," analyzes the failures of the SIN and of the entire intelligence system in its fight against terrorism. He criticizes in particular the use of intelligence by police within the Ministry of the Interior. Furthermore, he finds that the SIN of the 1980s experienced years of bureaucratic stagnation. The military continued to dominate national intelligence during the first Alan Garcia administration (1985–1990) as two army officers led the SIN during his regime.

The Political Police (Andean Stasi) and the Predatory State: 1991–2000

With the aim of reorienting Peruvian intelligence, the Alberto Fujimori administration introduced dramatic changes to the National Intelligence System in 1991. The instrument used was the highly controversial legislative decree 746, designed by the office of the Legal Advisor to the SIN (OTAJ-SIN). Longtime employees of the intelligence agency from the 1960s as well as the 1980s also participated in drafting the decree.

The legislative decree attempted to create an intelligence agency resembling Cold War intelligence services of Eastern Europe. Thus, one can think of this edition of the SIN as an Andean *Stasi*, from the name of the infamous East German intelligence enterprise.[73]

The justification for this intelligence design rested on its "centralized unity of command," and it became known as the "centralized management model." The model aimed to stem fragmentation of the National Intelligence System, a problem dating back to 1984. In retrospect, and "in contrast to the secret services of other democratic countries," the Peruvian SIN of the 1990s "was the leading institution in the power politics of the state."[74] Luis Piscoya

Salinas, a lawyer and analyst for today's National Strategic Intelligence Directorate—Internal Affairs of the National Intelligence Center (CNI), has critiqued the centralist model of Peruvian intelligence.[75] The CNI itself has not escaped his criticism.

The collegial Senior Intelligence Council (CSI) remained valuable for its role in interagency coordination. However, the new lineup of intelligence institutions in 1991 and 1992 excluded the council. The CSI had held the SIN in check until this time. But now the SIN was in charge of all of intelligence—like the SAVAK of the Shah of Iran or the political police of the respective communist parties of the Eastern Bloc. The SIN was everywhere.[76] The capture of terrorist leaders in 1992, 1993, and 1994 contributed to reinforcing its image as a successful model of centralized intelligence. It appeared clearly superior to the error-prone institutions of the 1980s, which were subject to more outside regulation. In addition, the centralized model brought into question the less centralized military approach, which had predominated during the 1980s.

In the 1990s, the SIN contributed decisively to the creation of the so-called predatory state.[77] Article 21 of Legislative Decree 746 (11 December 1991) revived the philosophy of Cold War Eastern European intelligence.[78] In the following year, a civilian self-coup originated by Alberto Fujimori brought on the promulgation of Legal Decree 25635. It was similar to the 1991 decree, except for some cosmetic changes.[79]

The Collapse of the National Intelligence Service (SIN)

Alberto Fujimori at one point asserted that the SIN was the best intelligence service in the world. However, he fell from power because he could neither control the SIN nor build his own political legitimacy. The SIN of the 1990s provided the key evidence that brought down the Fujimori administration. On September 14, 2000, Congressman Luis Iberico and others revealed the infamous Kouri-Montesinos videos unearthed from deep within SIN archives. The videos documented the SIN's bribery of elected officials on behalf of the Fujimori administration. The impact of this event destroyed the SIN and the authoritarian political regime that had employed the intelligence services precisely for the regime's self-preservation.[80]

Alberto Bolivar Ocampo, who was a SIN employee in the 1990s—along with the author—describes the organization:

> Between 1990 and 2000, Alberto Fujimori and Vladimiro Montesinos transformed Peruvian intelligence into a very efficient, internally focused political espionage machine, with control over communication channels and individual and collective spirits, totally subverting legitimate intelligence ends … the armed forces and national police became the chief threat to national security in Peru … as inside the country, intelligence carried out work that was foreign to its true purposes ….[81]

The Fujimori administration deactivated the SIN by an executive order and a special law (PL 461-2000/CR). The special law became standard Law 27351 in October 2000. Article 6 of this law expressly repealed Law 25635 of 1992. The Fujimori administration tried to maintain control of state intelligence in 2000. Mediation between the government and its opposition imposed by the Organization of American States forced the administration to create a new legislative proposal. This proposal (258-2000/CR) called for a National Intelligence Office, although the law was erroneously presented as an "organic" law rather than as a standard statute.[82] The proposal suggested the establishment of a Consultative Council for Intelligence to coordinate the efforts of the National Intelligence System. This proposed council resembled the abandoned Senior Intelligence Council that existed from 1984 to 1991. This initiative to sustain the SIN involved two urgent decrees (18 and 46, February and April 2001) in a final effort to allow the continued production of intelligence for the administration.

Improvements Attempted: 2000–2012

Successive political administrations undertook initiatives aimed at reconstructing the Peruvian intelligence system, ultimately without success.[83] The attempts failed despite honest and well-intentioned intelligence leadership in three consecutive administrations: those of *Accion Popular* in the transition period (2000–2001), *Peru Posible* (2001–2006), and *APRA* (2006–2011).

The Peruvian human rights and racial discrimination ombudsman (*Defensoría del Pueblo*)[84] took note of the turbulence and in 2001 formulated proposals for an intelligence service with democratic controls. It sought to avoid the intelligence excesses impinging on human rights.[85] The proposals came from the ombudsman's Group for Constitutional Affairs, which sent a version of them to the Intelligence Working Group set up by the Organization of American States in Lima. This group recommended certain safeguards for incorporation into a future intelligence law. The group also suggested that a congressional committee be responsible for intelligence oversight and control. It further stipulated that the National Defense Committee for Internal Order was not the appropriate place for that responsibility.

Based on five legislative initiatives by the transitional administration of Valentin Paniagua Corazao, Peruvian Law 27479 (2001) put in place the National Intelligence Council (CNI) and the National Strategic Intelligence Directorate (DINIE). For the first time, Peruvian intelligence was regulated by an ordinary law promulgated by the Congress of the Republic. The law (article 36) began to address congressional oversight of intelligence.[86] The oversight was limited to reviewing budget execution by the intelligence services. The legislation bore a striking similarity to Decreed Law 25635 of 1992, which had established the intelligence-centric, predatory state.[87]

Meanwhile, the executive branch instituted an "Annual Operational Plan," now known as the "Annual Intelligence Plan," which the congressional committee would check and approve, and then oversee in its implementation phase. Other elements of intelligence supervision provided for public transparency, safeguarding of information, and implementation of the concept of secrecy,[88] together with regulations on the handling of classified information. A Law of Transparency and Access to Public Information (2002) reinforced these principles.

In 2002, the Harvard University program in Peru, *Justice in Times of Transition*, convened in Lima. The journalist Juan Velit, director of the National Intelligence Council, presided. A working group prepared a report titled "Recommendations for the Reform of Intelligence in Peru in Light of the Experiences of Other Countries of the World." The project brought together international experts to study the strengths and weaknesses of intelligence-related legislation generated in democracies. Some participants pointed out

the inadvisability of having a law covering intelligence operations in Peru that was essentially a copy of the infamous Laws 25635 and 27479 of 2001.[89]

This was not the only sign of a reversion to the authoritarian state of 1991. Article 9 of the 1991 Law 27479 stated: "Both the private and public sector will provide to the National Intelligence System (SINA) any information needed for national security and national development." It did not specify how the SINA would obtain the information presumably necessary to ensure national security. Article 9 of this law reflected the influence of Legislative Decree 746 of 1991, in particular article 21, which established the information-collection tactics of the political police in communist Eastern Europe, such as the East German *Stasi*, the Romanian *Securitate* of Nicolae Ceaucescu, or the *NKVD* (precursor to the KBG) of Joseph Stalin in the former Soviet Union.

Politicians and intelligence leaders chose not to change the prevailing treatment of intelligence services. They did not develop public regulations to guide the application of Law 27479 of 2001. Even in the new, democratic regime, the detailed implementation of the intelligence law would remain secret.

Starting in 2002, various legal initiatives attempted to modify and improve Law 27479. The interest of legislators in reorienting the legislation was finally evident. A new presidential administration in 2003 continued the trend toward forging a new legal basis for intelligence. Initiatives emerged from several congressional committees, including National Defense, Internal Order, Intelligence, Alternative Development, and Countedrugs, to discuss issues that in the end might be incorporated into drafting a new national intelligence law.

The Ministry of Justice took a detailed approach to judicial control of intelligence operations. In addition, a special committee from the executive branch, acting through Resolution 097-2004-PCM,[90] developed the concepts of democratic control of intelligence, its legitimation, transparency, and accountability.[91] This committee drafted new intelligence legislation that envisioned a Strategic Intelligence Agency (AIE). The executive branch adopted the plan. The draft legislation applied regulatory principles to intelligence and laid out a structure for an independent congressional committee to address the intelligence function. However, in the end this initiative failed.[92]

The Peruvian Congress enacted the National Defense and Security Law (28478) in 2005, giving legislative approval to the intelligence system (SINA). Chapter 3, article 14 of the law notes that "the National Intelligence System is a part of the National Defense and Security System and is to produce intelligence and carry out those counterintelligence activities that are required for National Security. It [SINA] will operate under its own law and implementing regulations."

The National Intelligence System Law (28664) was promulgated in January 2006, establishing the National Intelligence Directorate (DINI).[93] The law included a provision for judicial control of intelligence "special operations." The definition of "special operations"[94] avoided the use of emotive words like "intrusive," "clandestine," "invasive," and "covert." In addition, Chapter 3, article 20 of the law explained in detail the judicial procedures for the execution of special operations:

- For the judicial control of special operations, the Supreme Court of the Republic is to assign two senior Justice officials for each case.
- Special operations require judicial authorization from one of the assigned Justice officials. The entire process will remain classified as secret.
- Requests to conduct special operations are made by the Executive Director of DINI to one of the senior Justice officials.
- When national security is endangered, and time does not permit preauthorization, the Executive Director of DINI may authorize a special operation, but must still seek approval of the Justice official, who within 24 hours can validate the request or order its immediate termination.
- The decision of the Justice official with respect to authorizing special operations is binding on all organizations, public and private, that may be associated with carrying out the operation, and all requirements for handling classified information must be observed.

- The request to conduct a special operation by the DINI, and the decision by the Justice official, are to be carried out within 24 hours, and are to be carried out by direct, personal interaction among those specific individuals.

- In the case of a negative decision by the senior Justice official, the appellant has the right to appeal the decision to the relevant court, which must resolve the decision within 24 hours.

The new intelligence law contained another notable stipulation: that the decision of the senior Justice officer to approve or deny special intelligence operations would not apply if the Peruvian Financial Intelligence Unit (UIF-Peru) were involved.[95] This provision was included to prevent the Peruvian Justice Ministry from restricting the functional, technical, and administrative autonomy of the UIF-Peru. The UIF-Peru solicits, receives, and analyzes information through Suspicious Activity Reports.[96]

The new law also called on the Peruvian Congress to create a Select Intelligence Committee that would exercise intelligence oversight independently from National Defense, Internal Order, Alternative Development, and Counterdrug Committees. Article 21 specifies the obligations of the Select Committee on Intelligence in such detail as to require an insider's understanding of congressional rules. Article 22 establishes the makeup of the committee: five or seven permanent members, either newly appointed or incumbent, with each new Congress. No backup or substitute members are allowed. Committee sessions are conducted in secret only if circumstances so dictate.

The leak of information from a component agency of the National Intelligence System, the Naval Intelligence Directorate, challenged the efficacy of the new intelligence law.[97] The cases known as MARTE-DINTEMAR (2007) and BTR (2009) infringed on the legal obligation to safeguard secrets during the handling of classified information.[98] The leaks occurred as military personnel undertook intrusive information activities while employed by private intelligence entities. The BTR case involved retired military personnel, but the activity undermined the principle that only the state has the right to obtain and deal with classified information.[99]

The Select Committee for Intelligence created a working group[100] under the leadership of Congressman Jose Urquizo (Nationalist Party). The Congress approved the group's report.[101]

Errors in Juridical and Institutional Processes Subsequent to the 2006 Intelligence Law

The Select Committee for Intelligence committed several errors during the 2006-2007 legislative season. The committee's first error was to consider itself a consumer or user of the intelligence product. The committee asked for "Information Notes," "Intelligence Notes,"[102] and "Special Intelligence Studies" from the National Intelligence system even though the legislative branch does not make decisions based on these reports. The committee legitimately oversees the intelligence system at the policy level, and debates and promulgates intelligence-related legislation.

The Select Committee also erred by contractually employing a set of advisers from the armed forces. Although supposedly expert in intelligence, these advisers lacked legal skills and an understanding of parliamentary practices. An example of the unfortunate results appears in the language of bill 2563/2007-R.[103] The bill contains some regressive proposals, to include:

- A legal formulation that proposed a vaguely defined "Central Directorate" for the National Intelligence System within the National Intelligence Directorate, reminiscent of the 1992 legal framework that gave unlimited intelligence license to Fujimori and Montesinos.

- Introduction, without explanation, of the term "covert actions," a concept beyond the scope of existing law. In addition, the bill refers to "reserved funds" in a way that appears to confuse this old concept with the new procedures for carrying out and funding special operations.

- A mixture of concepts related to the Select Committee, made without regard to congressional rules, which lay out both the principles and actions to be taken by congressional committees.

Not all aspects of congressional activity on intelligence matters are so regressive. The secondary set of committees responsible for intelligence legislation (National Defense, Internal Order, Alternative Development, and Counterdrugs) prepared a well-designed bill in 2010. Their bill (2563) corrects some aspects of intelligence law. Both proposed bills, sponsored by the Select Committee for Intelligence, were to be debated by a plenary session of Congress.

These developments show that parliamentary procedures and military interests figure prominently in the evolution of intelligence organizations and intelligence legislation, as various changes to the status quo are proposed and challenged.

Growth of Intelligence Control and Oversight in Latin America and Spain

Judicial control and congressional oversight provisions of the 2006 Peruvian intelligence law grew from earlier intelligence legislation created by Brazil, Argentina, and Chile.[104] By 2006, a broad regional foundation for intelligence law and legislation had emerged (see Table 1).

Table 1
Notable Intelligence Legislation, 1999–2005

Country	Law	Name of Agency	Year
BRAZIL	Law 9883	Brazilian Intelligence System (SISBIN)	1999
ARGENTINA	Law 25520	Intelligence Secretariat (SI)	2001
SPAIN	Organic Laws Number 2 and Number 11	National Intelligence Center (CNI)	2002
CHILE	Law 19974	National Intelligence Agency (ANI)	2004
MEXICO	National Security Law	Center for Research and National Security (CISEN)	2005
GUATEMALA	Legislative Decree 71-2005	General Directorate for Civilian Intelligence (DIGICI)	2005

Source: Compiled by the author.

Some common elements appear in national intelligence laws in the region. The elements include an imposition of external control over the intelligence services; the initiation of political checks and balances among all branches of government in applying external control; and an application of principles of public transparency and accountability. At the same time, expanded public accountability for government actions and greater transparency of intelligence management have shed light on and promoted the professionalization of this peculiar government function.[105]

Improvements in Public Control of Intelligence Across the Region Since 2006

Since the promulgation of the Peruvian national intelligence law in 2006, a series of legislative proposals in various countries point to more effective oversight and supervision of intelligence activities.[106] In some cases, executive branch budget processes reinforce the external controls applied by legislatures and judicial bodies. Budget processes can bring change to intelligence services through financial rewards and penalties.

Panama

Executive Decree 9, promulgated on 20 August 2008, reorganized the National Defense and Public Security Council and created the National Intelligence and Security Service (SENIS).[107] Title 5 of the measure established legislative and judicial control over intelligence services. Although rescinded because of irregularities in its promulgation,[108] the decree nonetheless contributed to recent comparative law in the region because it established the principle of "prior judicial approval" of legal measures that affect citizen rights. Judicially preapproved intelligence operations cannot be challenged or used as evidence in judicial or administrative court proceedings.

Colombia

On 5 March 2009, Law 1288 established rules to strengthen the legal framework for intelligence and counterintelligence, permitting those organizations to carry out duties in accord with the national constitution.[109] Chapter 3, article 13 of this law addressed intelligence control and supervision, specifying congressional oversight by a "Congressional committee to oversee intelligence and counterintelligence activities."[110] The law remained in limbo, however,

because of procedural disputes. Two supplementary laws (bills 189-2009 and 195-2011) would create a legal basis for ongoing intelligence activity in the country, pending the resolution of uncertainties with respect to Law 1288.[111]

By November 2011, a new Colombian National Intelligence Directorate (DNI) began to carry out intelligence activities, with the specific exception of "police" activities.[112] In addition, a DNI inspector general will ensure compliance with the law, examine the efficiency and efficacy of intelligence operations, and guarantee fulfillment of congressional committee stipulations.[113]

Ecuador

Ecuador replaced its legal framework for national security, the National Intelligence Directorate (DNI), by abrogating the National Security Law of 1979. On 15 May 2008, the Rafael Correa administration created a "Commission for the investigation of Ecuadorian military and police intelligence services." The intent of this investigation was not to pit military or paramilitary against civilians, but to address the problem exposed by the "Angostura incident"[114] wherein unauthorized links were discovered between those services and foreign intelligence organizations.

Executive Decree 1768, of 8 June 2009, created the National Secretariat of Intelligence (SENAIN), and the new Law for Public and State Security (Number 35 in the Official Registry, 28 September 2009). This last statute established rules for judicial authorization of "covert operations" in information collection and a plan for accountability to the National Assembly (Congress) by the SENAIN leadership and the highest authorities of implementing agencies.

Uruguay

In Uruguay, Representative Jose A. Amy (Colorado Party) presented a bill in June 2010 calling for the establishment of a congressional "Committee for the Supervision of Intelligence Services." Article 4 of the bill introduces specific principles[115] that intelligence officials should follow in collecting and handling information. The obligation to maintain secrecy is stated in article 5. The committee will follow rules for plurality and proportionality, and will include all political parties represented in the legislature. The bill's statement

of purpose specifies how the proposed intelligence law, for which no antecedents exist in the country, be developed. Political and technical participants will define sensitive aspects of national defense and security and ensure democratic protections of citizens.

Venezuela

Venezuela's attempt in 2008 to impose a controversial intelligence law, derisively labeled the "rat-out law,"[116] had so few constitutional and legal protections that the Chavez administration rescinded it. In its wake, Decree 7453 of June 2010 created a new intelligence organization, the Bolivarian Intelligence Service (SEBIN).[117] SEBIN replaced the political police of the Directorate of Intelligence and Prevention Services (DISIP). Intelligence laws of the Bolivarian Republic of Venezuela under Hugo Chavez resemble those of 1990s Peru, under Alberto Fujimori and his intelligence director, Vladimiro Montesinos.[118] The resemblances extend to aspects of style, background, and format.

Bolivia

Since early 2010, Bolivia has wrestled with how to create a Plurinational Intelligence Directorate (DIDEP) as a new type of organization to support political-strategic decisionmaking. A preliminary version of the measure envisioned an internal auditor. The plurinational Congress would oversee operational intelligence activities through a special committee, and the Bolivian comptroller would address intelligence administrative tasks. Fundamental civilian rights and protections would be guaranteed, and intrusive actions by intelligence services would not be permitted without judicial authorization. As a nominally civilian organization, the DIDEP would end the tradition of having the police and armed forces carry out all intelligence activities.

Conclusion

To answer the central question posed in this essay, the application of external controls (congressional, judicial and economic-financial) in Latin American has produced a decentralized model of intelligence. Peru's intelligence Law 28664 reflects the tendency toward decentralization. However, an innovation in Colombia may indicate a concurrent, centralizing tendency. There, an inspector general for the new National Intelligence Directorate provides

intelligence services with an opportunity to acquire some operational autonomy through the expedient of internal oversight. Autonomy contributes to a centralized model of intelligence activity.

The evolution of the centralized model, as well as decentralizing control and oversight mechanisms, has coincided with fewer violations of human rights by intelligence services. External control mechanisms have brought intelligence activities in line with democratic tendencies and values. This result is due mainly to intelligence system reorganizations across the region.[119]

Accompanying the reorganization of intelligence agencies, special executive or legislative commissions have institutionalized democratic reforms. The commissions have had some success in creating external controls over intelligence activities.[120] External controls ensure due attention to human rights, make judicial authorization of "special operations" standard practice, and establish democratic oversight of individual intelligence agencies. The commissions have allowed public discussion and systematic debate, thereby ensuring "social control"[121] by democratic constituents and collective public opinion.

Peru continues to face narcotrafficking, remnant terrorism,[122] and organized crime. Managing the tension between decentralized intelligence and intelligence autonomy remains a requirement for the effective work of preventive, secret services.

Addendum

In December 2012 the Peruvian government promulgated Legislative Decree 1141 on the Strenghening and Modernization of the National Intelligence System (SINA) and the National Intelligence Directorate (DINI). The Peruvian congress had granted the executive branch authority to draft legislation for the reform of the National Security and Defense System. Following similar initiatives in 1984 and 1991, this arrangement continued legislative-based regulation of all the country's intelligence agencies. The congress also designed, debated, and approved the earlier intelligence laws, Ordinary Laws 27479 of 2001, and 28664 of 2006.

The idea of authorizing the executive branch to design intelligence legislation came from a recommendation by the Congressional Intelligence Committee.[123] It originated with the first Congress (2011–2012) of the 2011–2016

congressional period, under the committee leadership of Congressman Jose Urquizo Maggia (of the ruling Partido Nacionalista/GANA PERU). In January 2012, Urquizo presented a package of five legislative proposals to modify existing Intelligence Law 28664.[124] All of the proposals were incorporated into the new legislative decree.

The new legislative decree, with its 6 titles and 43 articles, leaves intact the public or "democratic" controls exerted by legislative and judicial authorities.[125] The principles that guide intelligence activity also remain in place, extending the letter and spirit of the preceding Law 28664 of 2006. Decree 1141 similarly follows the lead of its antecedent law in presenting a glossary of intelligence concepts (in article 2) to improve the operation of the intelligence system and to establish the duties and responsibilities of each of the entities that make up the system. In this way, the decree follows the innovative Argentine Intelligence Law 25520 (2001).

Another feature of the new decree appears in its Title 5, "Measures for the Protection of Intelligence and Counterintelligence Personnel" (articles 38, 39, 40, and 41). These measures build on Bill 724/2011-CR, which proposed to "guarantee the physical integrity and security of personnel who participate in intelligence and counterintelligence activity." This bill was presented in Congress on 19 January 2012. Given their sensitive work in collecting human-source information (HUMINT), intelligence personnel benefit from specific legal protections. In Latin America, these safeguards also appear in Panama (Decree 9 of 2008), and in Colombia (Law 1288 of 2009).

Peruvian intelligence operates in a historically complex environment, characterized by both advancements and setbacks. With its new law based on a legislatively backed decree, the country has added a new wrinkle to intelligence oversight in the region.[126]

Andres Gomez de la Torre Rotta.
Lima, Peru, January 2013.

Andres Gomez de la Torre Rotta is a Peruvian lawyer, with a master's degree in international political economy (*Universidad de Belgrano*, Buenos Aires). He is a graduate of the Center for Hemispheric Defense Studies (CHDS), Washington, D.C., and has completed postgraduate coursework in Spain (political

science, international law). He is a former director of National Foreign Intelligence (CNI), 2001; former congressional adviser for the National Defense, Internal Order, Intelligence, Alternative Development, and Antidrug Committees; and for congressional investigatory committees (2002–2007). He has also served as director (2007-2009) of the National Intelligence School and faculty member (2007–2011). Additionally, he has served as an associate member of the Institute of International Studies of the *Pontíficia Universidad Católica del Perú*. He has participated in conferences on peace, security, defense, and intelligence in Quito (FLACSO), Brasilia (Brazilian Association of Defense Studies), and Rio de Janeiro (Social Cooperation Agency-Brazil and SIPRI-Switzerland). Gomez has also served as a member of Task Force–Peru Group, in the Cooperation and Regional Security Program of the Friedrich Ebert Foundation. He is an author for the anthology *Inteligencia Estratégica y Prospectiva*, published by FLACSO-Ecuador (2011), and *Cuestiones de Inteligencia en la Sociedad Contemporánea*, published by Spain's Ministry of Defense (2012). **Email:** *Andres_gotorrer@yahoo.es*.

Arturo Medrano Carmona, a Peruvian, holds a politial science degree from the *Universidad Nacional Federico Villarreal* and is a research assistant there. He is also a graduate of the Peruvian Advanced Studies Center (CAEN). He has participated in the online strategic game Nation Lab, organized by the U.S. Southern Command for CAEN. He is a specialist in administrative law and administrative procedures, Lima Law College.

Intelligence Laws of North, Central and South America

Liza Zuniga

Table 2 – Intelligence Laws of North, Central and South America			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
Argentina	Law 25520, enacted 3 December 2001. National Intelligence Law.	National intelligence is activity involving the collection, compilation, systematization, and analysis of specific information about actions, threats, risks, and conflicts that affect the exterior and interior security of the Nation (Law 25520, Article 1).	a) Secretariat of Intelligence, in the Office of the President. b) National Directorate of Criminal Intelligence, in the Ministry of Public Security. c) National Directorate of Strategic Military Intelligence, in the Ministry of Defense .
Brazil	a) Law 9883, 12 July 1999, established the Brazilian Intelligence System, created Brazilian Intelligence Agency, along with state agencies. b) Decree 3695, 21 December 2000, created Public Security Intelligence Subsystem. c) Decree 4376, 13 September 2002, set up the organization and functions of the Brazilian Intelligence System.	The activity having as its purpose the collection, analysis and dissemination of knowledge, inside and outside the national territory, about actions, and situations having immediate or potential influence over governmental actions or decisions, or the safety and security of the society and the state (Law 9833, Article 1, Number 2).	a) Brazilian Intelligence Agency (ABIN), principal organization, subordinate to Brazilian President. b) Brazilian Intelligence System, made up of nine Ministries (through separate organizations), plus a Comptroller, ABIN, Operational Command Center of the Amazon Protection System, and the Institutional Security Cabinet of the Brazilian President.
Canada	CSIS Act, 1984.	Security intelligence is information formulated to assist government decision makers in developing policy.	Canadian Security Intelligence Service (CSIS), lead agency for national security, reports to parliament through the Minister

Table 2 – Intelligence Laws of North, Central and South America (continued)			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
Canada		Regardless of the source of intelligence, it provides value in addition to what can be found in other government reports or in news stories. Intelligence conveys the story behind the story.	for Public Security. Other agencies: Bureau of Intelligence Analysis and Security and Bureau of Economic Intelligence within the Department of Foreign Affairs and International Trade, Communications Security Establishment, Canadian Forces Intelligence Branch, Criminal Intelligence Service, Financial Transactions and Reports Analysis Centre, Royal Canadian Mounted Police, Canada Border Services Agency, Chief of Defence Intelligence.
Chile	National Intelligence System Law 19974, 27 September 2004, created the National Intelligence Agency.	The systematic process of collection, evaluation, and analysis of information for the purpose of producing useful knowledge for decision making (Law 19974, Article 2).	a) National Intelligence Agency; central organization subordinate to the Minister of the Interior and Public Security. b) Defense Intelligence Directorate of the National Defense Staff. c) Intelligence Directorates of the Armed Forces. d) Directorates or Headquarters of Intelligence of the Forces of Public Security and Order.
Colombia	Law 1621, enacted 17 April 2013. National Intelligence Law.	Intelligence and counterintelligence develop specialized organizations, using human or technical means, to collect, process,	The Joint Intelligence Council (JIC) is responsible for producing intelligence estimates for the national government. This Council is made up of:

Table 2 – Intelligence Laws of North, Central and South America (continued)			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
Colombia		analyze and disseminate infomation, with the objective of protecting human rights, preventing and combating internal or external threats to the democratic way of life, to security, and to national defense, and complying with other objectives of this Law (Law 1621, Article 2).	a. The Minister of National Defense. b. The Senior National Security Advisor. c. The Vice-Minister of National Defense. d. The Chief of Joint Intelligence, representing the Commanding General of the Armed Forces. e. The Chief of Intelligence of the Army, representing the Army Commander. f. The Chief of Intelligence of the Navy, representing the Navy Commander. g. The Chief of Intelligence of the Air Force, representing the Air Force Commander. h. The Director of Police Intelligence, representing the Director General of the National Police. i. The Director of the Financial Information and Analyisis Unit, or his delegated representative. j. The Director of any other intelligence or counterintelligence organization authorized by by Law to carry out these activities.

Table 2 – Intelligence Laws of North, Central and South America (continued)			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
Colombia			The organizations that carry out intelligence and counterintelligence activities are those subordinate to the Armed Forces and the National Police, the Financial Information and Analysis Unit (UIAF), and the other organizations designated by law.
Ecuador	Executive Decree 1768, 8 June 2009, created the Intelligence Secretariat. Law on Public and State Security, 28 September 2009.	The activity of gathering, processing, and analyzing specific information on threats, risks, and conflicts affecting national security. Intelligence information supports security-related decision making (Article 14 of the Law on Public and State Security).	The Secretariat of Intelligence is the lead office of the National Intelligence System. It is made up of: a) Military Intelligence Subsystem, for national defense. Police Intelligence Subsystem, for internal security. b) Internal Security Management Office of the President of the Republic. c) Other intelligence organizations to be created or included in the future. d) Other institutions and organizations that have or produce information of interest for the purposes of ensuring state security.

Table 2 – Intelligence Laws of North, Central and South America (continued)

1. Countries with an Intelligence Law and Intelligence System

Country	Law	Legal Definition of Intelligence	Principal Organizations
Guatemala	Decree 71, of 2005. Law for the General Directorate for Civilian Intelligence (DIGICI), and Decree 18 of 2008, Framework Law for the National Security System.	Although the law does not include a definition of intelligence as such, it asserts that DIGICI has among its responsibilities, "to plan for, collect and obtain information, to process and systematize and analyze it, thereby transforming the information into intelligence." (Decree 71-2005, Article 3).	National Intelligence System is part of the National Security System, and is made up of: a) Secretary of Strategic Intelligence. b) Office of Civilian Intelligence of the Ministry of the Interior. c) Intelligence Office of the General Staff for National Defense of the Ministry of National Defense.
Honduras	Legislative Decree 211-2012, 15 April 2013, created the National Directorate for Research and Intelligence (DNIE) as an independent, nominally civilian organization responsible to the National Security and Defense Council. The decree also established a National Intelligence System, with a policy-level Strategic Intelligence Committee.	The DNIE protects the rights and freedoms of citizens and residents, prevents and counters internal and external threats against constitutional order, and implements public policies in defense and security as established by the National Security and Defense Council.	DNIE coordinates the National Intelligence System and chairs its Strategic Intelligence Committee. System members include: a) Honduran Armed Forces; b) Honduran National Police; c) Secretary of State, Office of International Relations; d) Financial Information Unit.

Table 2 – Intelligence Laws of North, Central and South America (continued)			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
Perú	Legislative Decree 1141, 11 December 2012. Law 28664 of 2006.	Activity comprising a systematic process of collection, evaluation and analysis of information, for the purpose of producing useful knowledge for decision making. (Legislative Decree 1141, Article 2).	The National Intelligence System (SINA) is a part of the National Security System, and is made up of: a) National Intelligence Council. b) National Intelligence Directorate. c) General Directorate of Multilateral and Global Affairs of the Foreign Relations Ministry. d) Defense: Second Division of Joint Chiefs of Staff of the Armed Forces; Intelligence Directorate of the respective Armed Forces. e) Interior: General Directorate of Intelligence of the Ministry of the Interior (DIGIMIN) and Intelligence Directorate of the National Police (DIRIN).

Table 2 – Intelligence Laws of North, Central and South America (continued)			
1. Countries with an Intelligence Law and Intelligence System			
Country	**Law**	**Legal Definition of Intelligence**	**Principal Organizations**
United States	The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-485. Executive Order 12333, 1981; Executive Order 13355, 2004; and Executive Order 13470, 2008.	National intelligence is information gathered within or outside the United States, that A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; B) involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security	National Security Council, Director of National Intelligence, National Counterterrorism Center, National Counterproliferation Center. Intelligence Community Organizations: Central Intelligence Agency, Defense Intelligence Agency, National Security Agency, National Reconnaissance Office, National Geospatial-Intelligence Agency, Department of State (INR), Department of Homeland Security, Department of the Treasury, Department of Energy, Federal Bureau of Investigation, Drug Enforcement Administration, Army, Navy, Air Force, Marine Corps, Coast Guard Intelligence.
Uruguay	A proposed law is being debated in the Uruguayan congress.* It is expected that the law will create a Secretary of National Strategic Intelligence, reporting directly to the president of the republic.	Intelligence acts on information developed in compliance with the principles of protection and defense of national, strategic interests.	The National Intelligence System will encompass the Secretary of National Strategic Intelligence and the Ministries of Defense, Interior, International Relations, and Economy.

Table 2 – Intelligence Laws of North, Central and South America (continued)			
2. Countries with Laws Affecting Information and Intelligence Agencies			
Country	**Law**	**Role of Civilian Intelligence Organization**	**Organizations**
Costa Rica	Law 7410 of 1994-General Police Law, and Executive Decree 23758 of 1994 address National Security and Intelligence Directorate.	The National Security and Intelligence Directorate will carry out intelligence operations that allow the collection and subsequent analysis of information as necessary.	Department of Police Intelligence of the Public Force. National Security and Intelligence Directorate.
El Salvador	Decree 554, 20 September 2001. Law of the State Intelligence Agency.	The responsibility of the Agency is "to inform and advise the president of the Republic on intelligence issues related to meeting national development objectives, the security of the state, and the viability of democracy" (Decree 554, Article 5).	State Intelligence Agency, subordinate to the President of El Salvador. Center of Police Intelligence, or the National Civilian Police. Intelligence Directorate of the Armed Forces Chief of Staff.
Mexico	National Security Law, 2005.	The purpose of CISEN is to produce strategic, tactical and operational intelligence that preserves the integrity, stability and survival of the Mexican state, supports governability and reinforces the rule of law. Its role is to warn of and propose preventive measures to dissuade, thwart and neutralize risks and threats that aim to harm the territory, sovereignty, constitutional order, freedoms and democratic institutions of Mexicans, as well as the economic, social and political development of the country.	The Center for Research and National Security (CISEN) is a civilian organization subordinate to the Office of the President. The Federal Police, the Army, the Navy and the Air Force all have intelligence offices.

Table 2 – Intelligence Laws of North, Central and South America (continued)			
2. Countries with Laws Affecting Information and Intelligence Agencies			
Country	**Law**	**Role of Civilian Intelligence Organization**	**Organizations**
Panamá	Law 15, 14 April 2010. It created the Ministry of Public Security (Law 9 of 2008 was repealed in 2010.)	None	To be determined by Ministry of Public Security.
Paraguay	Pending law (as of July 2014) will create a "national intelligence system."	Unknown	To be determined.
Venezuela	Decree 6865, 11 August 2009; Decree 8792, 31 January 2012; and other pending decrees to bring clarification to original decree 6068 of 14 May 2008.	The purpose of the Bolivarian National Intelligence Service (SEBIN) is to plan, formulate, direct, control, and execute civilian intelligence and counterintelligence policies and activities. It actions will be based on principles of honesty, participation, promptness, efficacy, efficiency, transparency, social responsibility, leadership in respecting human rights, ethics, political pluralism, and complete submission to law (Decree 7453, Article 2).	SEBIN is subordinate to the People's Ministry for Interior Relations and Justice. Intelligence branches of the Joint Bolivarian Armed Forces are subordinate to the People's Ministry for Defense.

Source: Liza Zuniga, with contributions from the editors.

* An Uruguayan newspaper report of 4 June 2013, "Actividad de Inteligencia estará regulada por ley," available at *http://www.republica.com.uy/estara-regulada-por-ley/*, is the source for the law's expected provisions as summarized here.

Watching the Watchers: Oversight of Intelligence Services in Democratic Regimes

Joanisval Brito Goncalves

"When oversight has been capable and constructive, it has been a major asset to the IC [Intelligence Community]. When degraded or misused, it has been an albatross around the neck of the intelligence agencies."

—Marvin Ott
International Journal of Intelligence and CounterIntelligence (Winter 2003)

Introduction

In modern democracies, government intelligence confronts existing threats and identifies opportunities to protect states and their respective societies from future threats. To attain national objectives, high-level decisionmakers need assessments of the kind offered by intelligence services.

Intelligence is not an agreeable activity for democratic states. According to Jose Manuel Ugarte, "it is not a commonly accepted activity, even if it is done on a daily basis and oriented outwardly; however, it does address the most important questions in foreign policy, economics and defense. Internally focused intelligence addresses threats capable of destroying the State and the democratic system."[127] A dilemma exists about the role of intelligence in democratic regimes: How can one reconcile the tension between the pressing need for secrecy in intelligence affairs and the equal need for transparency in government operations?

Democratic societies that experienced authoritarian periods in the recent past (such as Latin America and Eastern Europe) now need to ensure that security and intelligence organizations observe democratic principles on the domestic scene. Those principles dictate that intelligence services avoid arbitrary actions and renounce any attempt to abuse the fundamental rights and freedoms of citizens.[128]

How societies address the dilemma of transparency versus secrecy is an indicator of the degree of development of democracy in the society.[129] In mature

democracies, the dilemma is by definition resolved through effective and efficient mechanisms of oversight and internal control, and especially, external control exercised by the legislative branch.

This essay seeks to analyze the relationship between intelligence activity, as developed in democratic regimes, and the various mechanisms developed for its control. The essay will address basic aspects of oversight and control of intelligence practices and the practical mechanisms available in a democracy to carry out those goals. The experience of various countries in developing legal and institutional guidelines for effective oversight will be explored. First, elements of what some call "the spy game" require brief explanation.

The Intelligence Tool

Although as ancient as human existence itself, the intelligence function remains largely *terra incognita* to outsiders. The lack of knowledge contributes to the permanent tension between secrecy and transparency. This matters when the resolution of national security issues depends in part on how the public perceives intelligence activity.[130]

For classroom purposes and sometimes for operational reasons, the subject matter of intelligence falls into three branches: intelligence (collecting and analyzing information to produce knowledge); counterintelligence (protecting one's own knowledge and neutralizing hostile intelligence agents); and intelligence operations (secret and intrusive means to obtain protected information).[131]

Intelligence services deal with information, and information (knowledge) creates power. Therefore, a leader who wishes to manage official business smartly and powerfully will make good use of intelligence services.[132] When this happens, whether in a democracy or an authoritarian regime, intelligence services themselves can become powerful. Intelligence services may at times apply their power in arbitrary fashion, even targeting the very state and society they are designed to protect.

Issues Related to the Control of Intelligence[133]

One of the foundations of a democratic regime is the exercise of citizen control (direct or indirect) over institutions and agents of the state. The Brazilian

jurist Meirelles associates democratic regimes with the application of efficient and effective "public administration" mechanisms.[134]

According to Meirelles, public administration exercises control through vigilance, guidance, and "correction that one government branch, department or authority exercises with respect to the bureaucratic behavior of a counterpart in another branch of the same government."[135] The term "internal control" refers to that applied by departments within a branch of government (as exercised by the *Corregidor-General* of the union in the administrative system of Brazil, or the auditor general or inspector general in Anglo-Saxon countries). In the present study, "external control" is that carried out by organizations outside of the executive branch,[136] namely the legislative or judicial branch. Additionally, the concept of external, popular control, refers to the right of an individual citizen or the collective citizenry to oversee the actions of the state.[137]

From the Anglo-Saxon perspective, "control" and "oversight" are distinct concepts. Whereas "control" refers to the daily acts of administrative management within the executive branch, "oversight" (*fiscalização*) is linked to the powers of the legislative branch to look into whether the executive (that is, the administration) has carried out its responsibilities in accordance with legal and constitutional principles.[138] The term "control," as used in the Anglo-Saxon world, would translate to *supervisão* (supervision) in Portuguese.

"Accountability" has meaning for both control and oversight of intelligence. In the Portuguese-speaking world, this word pertains to the idea of "rendering accounts." In the realm of Anglo-Saxon public service, "[a]ccountability is an information process whereby an agency is under a legal obligation to answer truly and completely the questions put it by an authority to which it is accountable (for example, a parliamentary intelligence oversight committee)."[139] No exact translation or equivalent term in Portuguese encapsulates the Anglo-Saxon concept of accountability.[140] This detail contributes to the manner in which Brazilian society has traditionally addressed the management of public affairs.[141]

Insofar as control involves setting legal limits by which an administration must abide, *fiscalização* refers to the legitimate power of certain institutions and authorities to certify the administration's compliance with the judicial-

normative framework, to include the principles that guide the administration itself.[142] The principal source of power in a democracy—the citizenry—drives the concept of accountability. This is true no matter what accountability may mean to public officials who must render an account of their own actions or of the actions of the entire administration collectively.[143]

Another Anglo-Saxon term—"review"— refers to a type of control carried out *ex post facto*. This essay considers "control" a generic term, and "oversight" a type of control carried out through a particular administration's tenure. A "review," in contrast, always occurs in retrospect. In terms of external control of intelligence carried out by the legislative branch, *oversight* is more common among presidential systems, while recurring *reviews* predominate in parliamentary systems.

In countries with recent authoritarian governments, the adjustment of the state's security services to a democratic regime depends on the development of efficient and effective mechanisms to control their activities. Control mechanisms not only reduce abuses by security services, but also modify organizational culture and the perception that civil society has of these institutions, their agents, and their activities.

Control of intelligence activity starts with legal directives but extends to the implementing institutions. The legal framework for control ranges from constitutional provisions for individual rights and guarantees and general limitations on the actions of governments, to laws and executive orders. Implementation depends on the internal rules of government organizations, codes of ethics, instructions and directives applied by respective intelligence agencies.

Each intelligence agency or office has its own means of internal control. Managers at the different hierarchical levels are responsible to ensure that intelligence personnel act in conformance with legal and constitutional norms, and in compliance with organizational directives.[144] Even in the most senior executive branch offices, far from the environment of intelligence agencies, control is exercised by inspectors-general and by the minister to which the intelligence services are subordinated.

Beyond the internal control exerted within the executive branch, external control can be exercised by the judicial or legislative branches, or by an

independent institution (in Brazil, for example, by the public prosecutor—*ministério público*). External control guarantees some balance among the three government branches, especially in presidential systems, by virtue of checks and balances. Finally, institutions of civil society—the press, civic associations, and other organized groups— exert "citizen control." Individual citizens also contribute to control. They can act by accusing intelligence services of irregularities or by appealing directly to the judicial system to seek redress for violations of citizens' rights.

Control of intelligence activities, then, can take place in any of four domains or levels :

- **Agency-level 1** (internal to a particular intelligence agency);
- **Internal-level 2** (carried out within the executive branch by non-intelligence entities of the administration and by the state ministry to which the intelligence agency is subordinated);
- **External-level 3** (exerted by the judicial branch, the legislative branch, or an independent entity such as the public prosecutor in Brazil);
- **Popular-level 4** (the responsibility of individual citizens or civil society organizations).

Difficulties in the Control of Intelligence

Glenn P. Hastedt identifies secrecy as an impediment to intelligence oversight and control.[145] Intelligence practitioners cannot reveal their activities (and sometimes not even their organizational affiliation) to the public. To do so would make them vulnerable to counterparts from other countries, to their adversaries, and mainly to their own operational targets.[146]

Hastedt also maintains that intelligence resembles an artisanal craft more than a methodical science. Hence, intelligence professionals demand autonomy in making analytical decisions, in planning and conducting intelligence operations, and in interpreting data. They have little confidence in the knowledge or competence of their "controllers" (consumers), especially if the latter or their advisers have not routinely interacted with the intelligence community.

Employees of organizations that engage in control or oversight of intelligence need to have knowledge (and even better, practical experience) in the realm of intelligence. This experience makes it likely they will know how to identify irregular behavior among intelligence personnel and agencies. Those who are to hold intelligence services accountable should know what questions to ask.

Hastedt notes with concern the disinterest of politicians in intelligence. There is consensus among the authors who study this topic that "intelligence does not win votes," but it can cause an election to be lost.[147] Therefore, politicians prefer not to be involved in the business.[148] This explains the reluctance of some legislators and even executive branch officials to become involved in intelligence affairs, which can lead to the absence of control or to its dilution.

Hastedt points to another problem in the control of intelligence: the fact that those involved have differing opinions about "the problem of intelligence." Whereas some see control as necessary to prevent intelligence services from engaging in illegal activities, others accept the idea that intelligence officials do not see certain actions as illegal, in view of what is at stake—namely, national security.[149]

Another analyst argues that however difficult the environment for control of intelligence, there must be some control, although not to the degree that it presents an obstacle for intelligence activity, which after all is essential to the state.[150] Intelligence remains a safeguard for national security, and ultimately, for state survival.[151] Beyond this, although control of intelligence may be imperfect, one cannot speak of a consolidated democracy if its intelligence services are not subject to oversight and control by elected governments.[152]

In terms of external control, especially as carried out by the legislative branch, intelligence becomes legitimate only when oversight officials become capable evaluators of these secretive governmental information organizations. This observation points to one of the several paradoxes of intelligence control.

Paradoxes of Control

Marina Caparini explores the variety of paradoxes inherent to the control of intelligence activity.[153] Four aspects of the relationship between intelligence and its controllers give rise to this paradoxical framework, no matter the type of public administration under examination.

The first paradox stems from the dependence of the controller on information furnished by the intelligence entity. Those who intend to control intelligence activity have to know what to ask to carry out their responsibility. Yet outside observers have little opportunity to develop the necessary, detailed knowledge. Politicians thus depend on the information supplied by the same intelligence services they pledge to oversee.[154] In the United States, this problem makes congressional oversight difficult, as Zegart shows in her recent work on external control of intelligence services.[155]

She identifies two institutional deficiencies among congressional oversight authorities: limited expertise in the area and uncertain power over intelligence agency budgets. It is as if the intelligence world were hidden by an invisible cloak, or, to quote Max Weber, "unelected agency officials invariably know more about their own organization and its policies than the elected representatives who oversee them."[156] She lists other deficiencies: the lack (or low number) of persons in Congress who have served in the Intelligence Community, even among the advisory staffs of the intelligence committees; and in general a lack of familiarity with this secretive activity. Finally, no independent groups exist in the Intelligence Community who could provide assistance to the legislators as they attempt to exercise control. The dependence of Congress on the information supplied by the intelligence services themselves is, then, absolute.

A second paradox appears when a controller becomes a significant advocate for, or a determined adversary of, the controlled. Either condition can have a great impact on the flow of information. An antagonistic relationship creates communications barriers and makes control more difficult. When controllers go too far in accommodating the controlled, oversight does not occur. This paradox may resolve itself with the maturation of democratic institutions, particularly if public servants become conscious of their role in oversight and apply democratic values to their work. However, ethical culture has to emerge to the point of changing institutional practices, never a simple process. Change comes slowly because intelligence oversight rarely interests legislators. Attention to intelligence oversight evokes negative emotion from voters as it diverts legislators' attention from more palpable issues that directly affect the lives of the electorate.

Another issue arises from the dichotomy of "functional control" versus "institutional control." Usually, oversight and control are accomplished as an institutional mandate; that is, the entities responsible for control oversee a range of institutions and not the activity itself. However, national security functions, including intelligence, are carried out in diverse agencies and departments of government. Institutional control risks leaving some agencies or departments without oversight. To resolve this problem, Whitaker suggests a reorientation from institutional to functional control. In this way, oversight would be accomplished in light of the activity of interest, irrespective of the organization that actually carries it out.[157]

Caparini's final paradox grows from excessive secrecy, which can lead to uncontrolled release of sensitive information. The paradox rests on three points: 1) secrecy promotes intelligence success, a public good; 2) restrictions on access to information inhibit public debate and social control initiatives; 3) intelligence services tend to "indiscriminately over-classify" or "overvalue" the knowledge produced, the sources used, and even the raw data collected, as they resist declassification of documents. All of these points reduce transparency and can lead to an "erosion of discipline" among intelligence officials.[158] Excessive restrictions on intelligence disclosure commonly generate an increase in intelligence leaks. Justifications for leaking range from a real preoccupation with illegality and the violation of democratic principles to personal interests (motivated, by example, by the individual's financial difficulties, discontent with an institution, or internal rivalries). Leaks are usually made to the press, as a guardian of transparency.

Even in the United States, where congressional oversight has a long history, legislators have little access to documents and knowledge produced by or in the possession of the Intelligence Community.[159] Zegart points out that the most important oversight organization, the Government Accountability Office (GAO), the equivalent of the Court of Auditors (*Tribunal de Contas*) of some Latin American countries, has been prohibited from undertaking audits of the Central Intelligence Agency and of other intelligence agencies on the grounds of protecting national security. This occurs despite the GAO's having more than 1,000 employees with access to top secret documents, and more than 70 authorized to review information at the highest level of classification—sensitive compartmented information (SCI). Legislators themselves

have limited access to these documents and their staff members may not access documents or knowledge held by the Intelligence Community. Thus, external control in the United States remains severely limited.

Oversight Principles Applied to Intelligence Activity

Each country of the region has its own distinct intelligence system and a mechanism for control and oversight suited to its culture and political traditions. Thus, Peter Gill asserts that it is not correct to suggest that states may simply choose to adopt a method of control existing elsewhere; political institutions cannot simply be transplanted from one system to another.[160]

Rather than simply copying an institutional model for oversight, a country should identify general principles and then implement particular procedures suited to its system of governance. According to Manuel Ugarte,[161] a thoughtful control of intelligence rests on responses to the following questions: What is to be controlled? Why, and for what reasons, is it necessary to control intelligence activity? How and by what means can control be exerted, and with what objectives?

Gill presents some general principles of control that apply to three of the four domains cited earlier: 1) agency, 2) internal (managerial) within the executive branch, and 3) external.

The first general principle asserts that managerial control and external oversight apply to all domains, except where popular control is exerted by citizens. Thus, where external oversight of individual intelligence agencies occurs (typically in congress), managerial control also takes place (for example, when Congress pre-authorizes an intelligence operation or approves resources for it).

A second general principle declares that whoever produces intelligence cannot engage in oversight of the activity. This does not mean that those who engage in intelligence operations should not consider the legality of their operations with respect to individual rights and freedoms. Beyond any established legal boundaries, deeply rooted ethical principles remain indispensable to guiding the actions of intelligence institutions. However, Gill considers it "naive to believe that ministers or officials will be able to subject their own actions to effective oversight."[162]

A third principle recognizes the obligation of those responsible for the oversight of intelligence services to establish clear behavioral standards and rules, and to make them available to the public without compromising security. These norms and standards (codes of conduct, directives, guidelines) become increasingly detailed as the focus of control moves to the internal environment of particular intelligence agencies. Judicial systems based on the Romano-Germanic legal tradition, in particular, require a normative framework. Brazil and other Latin American countries share this legal tradition.[163] Without clear laws to guide and limit the actions of intelligence and security services, the risk of abuses is high in these systems. The risk of abuse elevates the importance of making these norms known to all citizens.

A fourth principle is related to political control of intelligence. Here, each "passive" official answers to an "active" official who sits at a higher level, and in the case of intelligence oversight, this chain begins inside individual intelligence agencies. For example, an intelligence agency or service (level 1) is passive with respect to the external control that an active (level 2) executive branch organization exerts. These hierarchical relationships fit comfortably with parliamentary systems, where a clear sequence exists in the transfer of authority from Parliament to the executive branch (Cabinet), and from there to the administrative bureaucracy. These relationships do not apply so clearly to presidential governments. Also, a level 1 organization is subject to simultaneous control by entities not only from level 2, but also levels 3 and 4.

A fifth principle requires that each controlling entity report to the executive authority at its own level. As Gill explains, an oversight office external to an intelligence agency must report to the ministry responsible for control at that level. In South America, the authority of one branch of government to control another, and the responsibility of the administration in power to be accountable to the ultimate source of power over state activities—the citizenry—often remains unresolved. It is not surprising that the Portuguese language has no word equivalents for the concepts of "accountability" and "enforcement."

The last principle identified by Gill highlights the need for broad cooperation between the organizations that control intelligence at different levels. This need becomes evident when there exists an intelligence community (a network[164]) that is controlled institutionally rather than functionally.

When controlling organizations cooperate and exchange information, they strengthen their oversight capability by acting as one. Without cooperation, oversight quickly fragments and becomes less effective. An effective control of intelligence networks depends on a networked approach to oversight, which is to say, the application of *functional* oversight.[165]

Gill's final observation is that organizations exercising control and oversight should have access, at least potentially, to all the information produced by intelligence and security services. That information should include details of specific intelligence operations. Only in this way can the bureaucratically "active" entities definitively complete their obligations. This ideal arrangement would signal an acceptance of the essence of "accountability."

Approaches to the Control of Intelligence Activity

This section examines some of the intelligence oversight practices now in place across the region. They may contribute to developing a legal framework for intelligence here or elsewhere. The author has drawn on familiarity with political and intelligence systems in Canada, the United States, and Western Europe, as well as some knowledge of the new democracies of Eastern Europe. Some examples also come from Latin America, where the administrative control of intelligence continues to gain strength.[166]

Separation of the Intelligence Apparatus into Different Organizations

An important practical mechanism to enable control, according to Thomas Bruneau and Kenneth Dombroski,[167] is to divide the apparatus into different agencies, so as to prevent a single entity from having a monopoly on the collection, production, and dissemination of intelligence. Typically, then, civilian and military organizations, police, and prosecutors, as well as distinct domestic and foreign intelligence agencies, share the responsibility of carrying out the function. Many countries, among them the United States, Israel, France, the United Kingdom, Germany, Portugal, and Russia, distinguish between external intelligence services and separate, internal security services.

Need for Institutional Clarity

The purpose of the intelligence agency or service needs to be clearly defined and limited to actions that can be explicitly detailed. All actions should relate

to serious threats to national security.[168] The territory for which each organization bears responsibility should also be defined, and its sphere of action outside of the national territory or jurisdiction should be accompanied by corresponding safeguards.[169] In countries with post-authoritarian regimes, legal and institutional guarantees deserve full public notification to prevent or stop inappropriate uses of the security or intelligence apparatus, to include the use of the intelligence apparatus against political opponents.

Accountability of Intelligence Service Leaders

The choice of who should lead the intelligence services matters because that individual will bear the responsibility for ensuring that the organizations conform with democratic principles and expectations. The legislature should establish a process for approving the nominee, as well as for specifying the professional credentials of candidates for the office. The factors that would disqualify a candidate from obtaining the post or remaining in it should also be identified. More than one member of the cabinet (or administration) should participate in the choice of candidates for intelligence director. Opposing legislative or parliamentary voices should also participate in approving the nominee. All this (especially the criteria for nomination, designation, and removal of the director) should be specified by law to avoid undue pressure on the director once he or she attains the office, and to ensure that the leader not act in an inappropriate or abusive manner.

Rules for Intelligence Data Collection, Handling, and Eventual Release to the Public

Democratic control of a security and intelligence establishment involves the collection of data, the production and handling of intelligence, and the use and disposition of information archived by the intelligence services. Regulations that restrict the use of current information and of intelligence archives should extend to the collection and handling of information about the private and intimate life of individuals. Further, rules need to guide the retention of information, the use of and access to archived information, and its ultimate destruction. Rules also need to address adherence to any international principles covering the protection of information, and provide for periodic audits to ensure compliance with laws and regulations.

Brazilian legislation covering access to intelligence information underwent significant changes in 2012. Law 12527, the Law on Access to Government Information (LAI), notably addresses public access to classified information.[170] Produced under the Third National Plan for Human Rights, the LAI emerged in parallel with the Truth Commission established to verify instances of human rights violations committed between 1946 and 1988 (bracketing the period of military rule, 1964–1985). The LAI adopted a strongly revanchist or vengeful approach. It gives little protection to state secrets because of a provision rescinding without review the "confidential" classification, making all of the information and documents created at this level available to the world through publication on the Internet. The LAI also establishes uncontestable, fixed periods for the release to the public of "reserved" documents (5 years), and "secret" documents (15 years). The law is more discriminating with respect to the release of "top secret" documents: they may remain classified for 25 years, with only one opportunity to contest their automatic release. If their release is successfully contested, they may remain classified for another 25 years.

Thus, any document produced or kept by the state can remain classified for, at most, 50 years. This means that all the data, intelligence, and any other official documents produced before 16 May 1962, should, after 16 May 2012, be released to anyone, with no specific justification or reason needed on the part of the requestor. Despite the popularity of this law in Brazil (even though the details of the law are not widely known or understood), a few critics do exist. The critics see the law as irresponsible in permitting unrestricted access to any and all information, including information that can compromise the interests of the state, putting it, or the society at large, at risk.[171]

Intelligence should not be excluded from the embrace of norms that protect and ensure the public's right to information, except for aspects of secrecy that relate directly to national security. The judicial branch should be able to examine the conduct of intelligence organizations, to include their recourse to special powers. In the case of the Brazilian LAI, article 21 expressly establishes that "access to needed information cannot be denied to judicial or administrative guardians of fundamental rights" and that "intelligence or documents that reveal conduct suggesting misconduct by public officials themselves, or

by order of public authorities, involving the violation of rights, cannot be withheld from investigators."

Certainly the implementation of laws governing access to information is not a simple matter. For example, in Mexico, the Federal Law on Transparency and Access to Public Governmental Information (published June 11, 2002)[172] encountered a series of difficulties upon implementation. One difficulty was that it only regulated access to public, governmental information at the federal level, leaving the 31 states and the Federal District the task of producing similar regulations at the state and municipal levels.[173]

Special Handling Rules Needed for the Products of International Intelligence Exchanges

Intelligence is increasingly exchanged with foreign security services, as well as with international organizations. The receiving side promises to retain the information and use it while observing the same safeguarding regulations established by the national legislature of the country or international entity that provided it. In the Brazilian case, the Law on Access to Government Information, despite the fact that its article 36 establishes that "the treatment of secret information resulting from treaties, accords, or international agreements will abide by the norms and advice contained in those instruments," does not spell out the handling requirements for classified documents produced as a result of the intelligence pursuant to any international agreements. This situation has led the International Relations and National Defense Commission (CRE) to suspend the negotiation of any agreements having repercussions on the security of sensitive information,[174] and to recommend to the executive branch the renegotiation of all existing agreements of this kind.[175] The Brazilian experience exposes the need for routine review of intelligence-handling practices to avoid international reproach.

Establishing Rules for Executive Access to Intelligence

To exert appropriate control over intelligence, executive branch officials need rules to guide their access to intelligence information. At the same time, it is also helpful for the leader of an intelligence organization to have access to the minister for whom he or she works. That minister, in turn, should be responsible for formulating security and intelligence policies. The Brazilian Intelligence Agency (ABIN) reports to the Institutional Security Cabinet (GSI)

of the President of the Republic. Law 9883 of 1999 establishes, in its article 9, that "any information or document produced about intelligence issues or activity, whether in draft form or fully in the custody of ABIN, may only be made available to those authorities who have a legal right to solicit the material, as established by the chief of the GSI."[176]

Moving beyond Ad Hoc Congressional Notification of Intelligence Operations

The control of very intrusive intelligence activity appropriately requires preapproval by an executive branch authority, in accordance with any relevant laws. Also, the legislative branch warrants notification of sensitive intelligence operations already underway and it occurs mainly in presidential systems of government. A good example comes from the United States, where notification goes to the "Gang of Eight," a group of representatives and senators who are credentialed for access to even the most intrusive and secretive operational activities carried out by intelligence organizations of that country.[177]

In the U.S. model, the president of the republic has the obligation to keep congressional intelligence committees completely and continually informed of all the most sensitive intelligence operations (covert actions), to include the decision to proceed with an action, and specifically before the action actually takes place.[178] When the president considers a specific operation vital to the interests of the United States, he can limit the prior notification to the Gang of Eight and to any other leaders of Congress he or she chooses to inform.[179] This occurred in the case of the exquisitely sensitive attack on the Osama Bin Laden compound in Pakistan.

Establishing Safeguards for Independent Mechanisms of Intelligence Control

When control is exercised by an independent authority external to security or intelligence organizations, but part of the executive branch (such as an ombudsman or an inspector general), the official needs to meet legal and constitutional requirements for the position. Additionally, to ensure his or her effectiveness, the independent authority should not be subject to removal from the position during the designated time period, should have legal powers sufficient to oversee and manage issues in depth, and the acumen to evaluate arguments related to the practices and nature of intelligence organizations.

The official should have authority to review the nature and application of any order, report, or decision that results from the process of oversight. The law should indicate the scope of this type of control, including to whom (or to what organization) the independent authority should report (for example, to the minister to which intelligence services are subordinated, to the controlling organization, or to the leader of the executive branch).

These suggestions provide safeguards against potential ministerial abuses of intelligence oversight arrangements. The legislature should establish the rules, and provide guarantees against the politicization of intelligence services. Mechanisms for establishing viable safeguards include: 1) a legal determination that all the orders, directives, and requirements of the minister be written and made known to an external reviewing organization; and 2) a legal provision that the minister keep the leader of the opposing political faction(s) informed of his principal actions and orders with respect to the intelligence services. Clearly, these recommendations and others that might follow may appear Utopian, but if implemented, they could promote useful changes to the manner in which secret services are controlled.

Recognizing the Tension between Apolitical Intelligence and Tracking Internal Threats

Safeguards may also prevent a situation whereby the intelligence services operate in favor of the interests of one party or political group. They should not engage in collecting information about acts of protest or dissension, a normal part of the democratic process when carried out in accordance with the law. However, intelligence services should not refrain from tracking organizations that, although legally established, represent or could come to represent a threat to democratic institutions, to national security, and to the society, to include social movements or political groups that endorse subversion, promote institutional instability to obtain political objectives, or that try to take political power by force. Canada has developed a unique strategy to ensure public accountability for such groups who try to use legal protections to avoid intelligence surveillance.

Ensuring Openness of Legal Contests Involving Protection of Sensitive Information

The judge or tribunal assigned to receive complaints and to judge actions must meet legal prerequisites for holding that office. Once confirmed to

office, these individuals should not be removed from the position during the designated time period, and need full legal authority to issue mandates or any pertinent type of order to achieve the intended results of the oversight process. Even as secrecy may characterize some judicial processes, all parties to legal contests involving sensitive information will enjoy procedural transparency. In Brazil, criminal and civil legislation guarantees access to all proceedings in support of a sound defense strategy. The new LAI does the same for legal contests involving the protection of information.

Legislative Centrality in Developing and Applying Control and Oversight

Congress (or parliament) offers the choicest examples of external control from a public administration perspective, and this is especially true in the case of intelligence activity.[180] In Brazil, congressional control of executive branch functions in general, and of the intelligence services in particular, are accomplished through three distinct instruments: required appearances before congress by ministers of the state,[181] formal requests for information,[182] and public hearings.[183] Each of these three measures is constitutionally based, and each is commonly employed, although the first is generally used to exert individual control,[184] whereas the latter two are oriented toward collective accountability. To control intelligence activity, from the time the law creating the Brazilian Intrelligence Agency was debated until the more recent crises involving intelligence institutions, such as the theft of laptop computers from *Petrobras* (Brazilian energy company) that may have contained sensitive information about Brazilian petroleum reserves, officials of the executive branch have been called to account in congress through public or private hearings, ministerial convocations, and formal requests for information.[185]

A congressional committee serves as an ideal vehicle to exert external control over an intelligence community as it reduces unnecessary confrontation with political interests. The committee can include representatives and senators or it can reside in just one of the two legislative chambers. Alternatively, two committees may be created, one in the lower chamber and one in the senate. In all cases, the committee needs a broad mandate, covering the entire set of intelligence organizations (including all departments and auxiliary activities and personnel). A broad mandate extends coverage to other, functional aspects of oversight: the legality, efficacy, and efficiency of intelligence, its budget and

accountability, and its compliance with national and international norms for the protection of human rights.

Legislation should mandate that congressional oversight bodies report only to Congress. This arrangement would help offset the influence of committee "subordinates" who act on behalf of the executive branch.[186]

Congressional oversight can focus on controlling the intelligence budget. Congressional organizations commonly have access to all intelligence budget documents, and they observe safeguards to deter leaks of classified information. Budgetary oversight of security and intelligence needs to obey principles of good government, with exceptions only as permitted or demanded by relevant laws. The most suitable approach to overseeing the intelligence budget joins the committee dedicated to intelligence oversight with the congressional budget committee. A strong legislature will exert full authority over budgetary matters, so that intelligence services may use resources only for specific, authorized purposes, and cannot transfer funds to a contingency account without legislative authorization.

All of the recommendations made here will certainly encounter resistance to implementation, with resistance coming from the organizations subject to oversight as much as from Congress itself. After all, congressional attention to oversight will insert representatives and senators into a politically delicate and disagreeable world with electoral repercussions. Rarely do legislative officials have an interest in intelligence activity, for various reasons.[187] In political-juridical systems with a strong Romano-Germanic tradition, major transformations begin with legislation that assigns clear mandates to intelligence organizations, their overseers and managers. Difficult change requires serious political will.

Pushing the Envelope: The Canadian Example of Independent Oversight

Canadian experience with intelligence control merits special attention for its pioneering approach. In 1984, this country created the Canadian Security Intelligence Service (CSIS), a civilian service oriented toward internal security, but with an additional mandate to undertake foreign intelligence in defense of Canadian interests. The law creating CSIS (the CSIS Act) also brought

into being an independent organization, the Security Intelligence Review Committee (SIRC), to carry out external control and review (not oversight) of the service. The SIRC reports to the Canadian Parliament.

The CSIS law appeared at a point in Canadian history when citizens were questioning some responsibilities of their government, in particular the role of the state in safeguarding individual freedoms and rights. Only two years earlier, in 1982, a new constitutional law had created the Canadian Charter of Rights and Freedoms to protect civil liberties and individual rights. The CSIS Act brought changes to Canadian intelligence practices and to public perception of the intelligence services. The national intelligence culture changed as the public debated the mission of intelligence services and the prerogatives of the state in protecting the security of citizens.

Simultaneously with the promulgation of the CSIS Act, parliament approved the Security Offenses Act, giving the Royal Canadian Mounted Police (RCMP) jurisdiction over issues of national security related to law enforcement. At the same time as worries about terrorism were growing, there was also growth in the number of agencies or departments with national security and intelligence obligations. Government intelligence activities related to national security did not remain exclusively under the purview of the CSIS.

The innovative CSIS Act made accountability, control, and review mechanisms explicit. The act dedicates all of its Part III—Sections 29 to 56 (of a total of 56 sections)—to the control of CSIS. The prerogatives and power of control reside in the executive branch of government as well as in parliament, where the SIRC operates. Part II of the CSIS Act (Sections 22 to 28) addresses judicial control of intelligence. Additional attention to accountability appears in other sections of the law as well. For example, the CSIS director must report to the minister of public safety, as well as to the SIRC, about any documents sent to the attorney general. The minister of public safety must also forward a copy of his directives to the CSIS director to the SIRC.[188] Therefore, much of the law's text (about two-thirds) attends to the different modalities of control of Canadian intelligence activity as conducted by the CSIS.[189]

The Security Intelligence Review Committee stands as the great innovation of the Canadian legislation. The SIRC mandate appears in Sections 38 and

39 of the CSIS Act. The SIRC conducts independent reviews of and regulates CSIS activities.[190] It assures parliament and Canadian society at large that the national intelligence service remains in compliance with its mandate to guarantee the security of the state and to preserve individual rights and freedoms. To that end, the SIRC monitors and reviews the institutional objectives of the CSIS and investigates any claims or complaints against the service.

The SIRC also ensures that CSIS observes the regulations and directives of the Ministry of Public Safety, and that the service not undertake its activities in an arbitrary, excessive, or unnecessary manner. At the same time, the SIRC prevents certain groups from using the protection of individual rights and freedoms as a shield to cover actions that threaten Canada or its allies.[191] Finally, the SIRC can examine the reports of the CSIS inspector general to double-check the facts behind particular issues before presenting its own conclusions and recommendations about the activities of CSIS.[192]

The SIRC also investigates two kinds of complaints: those related to "any activities of the intelligence service," and those indicating a decline in the trustworthiness of public servants, candidates for public office, or contract employees with the government.[193] Accusations may also be addressed by ombudsman-like commissioners. Specific commissioners whose jurisdictions relate to security and intelligence are those for the Communications Security Establishment (CSE) and the RCMP.

Improving the accountability of national intelligence systems depends on the adoption of efficient and effective mechanisms for the oversight and control of intelligence activities. Naturally, not all of the suggestions presented here will fit a single model of government.

Conclusion

Societies that have recently emerged from authoritarian periods often view intelligence with suspicion, fear, or even hatred. Intelligence services have often served as part of the repressive apparatus of a dictatorship. This relationship has distorted the subsequent perception of the intelligence role in the defense of state and society.

Structural problems in Latin America intensify the effect of paradoxes in the control of intelligence activity. These problems relate to an authoritarian

history in several countries, where the intelligence apparatus supported the governing authorities. In addition, the Romano-Germanic and positivist structure of judicial systems in much of Latin America dictate that changes can be made to intelligence control mechanisms only upon the implementation of new legislative frameworks. In this environment, two paths toward reform may be expected, neither of them very promising.

First, legislative inertia and insufficient societal interest in bringing pressure to bear on legislators mean that new laws in the area of intelligence cannot easily be advanced and approved. One consequence is that the issue of control remains without sufficient regulation, whereby existing laws permit only a low level of congressional control, and at the same time leave a great deal of discretionary power in the hands of the intelligence services.

A second scenario foresees that new laws, in practice, will have little effect. In this case, a superficial layer of legality limits enforcement of intelligence control measures by the judicial system. This has happened in Brazil, where, despite legal provisions for an external control organization in congress, the legislation has given insufficient support to the exercise of oversight. In addition, little political value comes from debating the control of intelligence services, resulting in correspondingly little involvement by legislators.

The fourth level of control over the secret services rests with the civil society, or the people. Popular control can involve organized groups of citizens (assembled, for example, in nongovernmental organizations, unions, or associations). On the other hand, a single individual may independently complain about the secret services. Popular control may come through freedom-of-information requests (facilitated by the Brazilian LAI, for example). The success of popular control measures directly reflects the level of democratic maturity in a country's institutions.

The exercise of oversight and control of the intelligence services does not occur automatically in a democracy. Even in the United States and Canada, where external control of intelligence services has become a decades-old tradition, questions remain about its effectiveness. Effective external control of intelligence requires sustained effort by legislators, a commitment they hesitate to make.

Without exception, however, having the intelligence services under control, and especially under external control, remains democratically healthier than continuing without positive institutional arrangements for the guidance of this government activity.

Author's Biography

Joanisval Brito Goncalves, a former intelligence officer with the Brazilian Intelligence Agency, now serves as a legislative consultant to the Federal Senate of Brazil, focusing on international relations and national defense. He also advises the Brazilian National Congress's Joint Committee on Intelligence Oversight (CCAI). He holds a Ph.D. in international relations from the University of Brasilia, and a specialist's certification in national intelligence from the Brazilian National Intelligence School (ESINT). As a lawyer and university professor, he has more than a decade of professional experience in the study of intelligence. He teaches at the Minas Gerais Public Prosecutor's Advanced School, the Army's Military Intelligence School, the National Police Academy (of the Department of Federal Police), the Brazilian Legislative Institute, and the Federal District's Advanced School of Law. His publications include *Atividade de Inteligência e Legislação Correlata and Políticos e Espiões—o controle da atividade de inteligência*, both published by Editora Impetus. The ideas and opinions expressed here are exclusively those of the author and do not necessarily reflect the positions of the organizations with which he is associated. He may be contacted at: *joanis@senado.gov.br or joanisval@gmail.com*.

Status of Oversight over Intelligence Services

Russell G. Swenson and Carolina Sancho Hirane

This table refers only to legislative and judicial procedures in place to oversee or control the domestic actions of intelligence services.

Table 3
Status of Oversight over Intelligence Services

Country	Legislative Provisions	Judicial Provisions
Countries with legislative and judicial oversight over all intelligence services		
Argentina	National Defense Law 23554 (1988)[194]; Bicameral Intelligence Committee of Congress, Law 25520, title VIII, articles 31-41	National Intelligence Law 25520 (2001), Article 5
Brazil	Bicameral Committee on Intelligence (CCAI).	Judges must authorize any sort of telephone tap conducted by police forces. The judiciary branch receives complaints against secret services. Public prosecutor controls the police forces, but a debate remains over whether the public prosecutor has powers to control just the criminal investigation or if these powers can be extended to police intelligence.
United States	Intelligence committees in both houses of Congress since 1976	Foreign Intelligence Surveillance Act (1978), with amendments
Countries with only judicial oversight over all intelligence services		
Colombia	Bicameral Intelligence Committee in Congress	None

Table 3 Status of Oversight over Intelligence Services (continued)		
Country	**Legislative Provisions**	**Judicial Provisions**
Countries with only judicial oversight over all intelligence services		
Costa Rica (only has national police; no military)	None	Decree 23758 (1994), Chapter 3, Article 13, withdrawn in 2005.
Countries with oversight, but not over military intelligence services		
Canada	Security Intelligence Review Committee (1984–present) Independent; reports to Parliament	Canadian Security Intelligence Service Act (1984), Part 2
Chile	Intelligence committee in the lower house of Congress	Law 19974 of 2004. Judges authorize special procedures for collection of information by intelligence services.
Ecuador	Special committee or Congress	Law on public and state security of 2009. Judges authorize special procedures for collection of information by intelligence services.
Guatemala	Special committee of Congress	Decree 71 (2005), Article 4
Honduras	None	Supreme Court will review accusations of invasion of privacy by the National Directorate of Research and Intelligence.
Mexico	Bicameral Intelligence Committee of Congress	National Security Law (2005), Title 3, Chapter 2
Panama (no provisions for oversight at present; see details in next columns)	Special committee of Congress (until Law 8 of 2008 was repealed in 2010)	Law 8 of 2008, Title 5, Chapter 2 (but now repealed)
Peru	Bicameral Intelligence Committee of Congress	Article 20.2 of Law 28664 (2005)

Table 3 Status of Oversight over Intelligence Services (continued)		
Country	**Legislative Provisions**	**Judicial Provisions**
Countries with no legislative or judicial oversight over intelligence services		
El Salvador	None	None
Nicaragua	None	None
Paraguay	None	None
Uruguay (law being debated in Uruguayan Congress 2013-2014)	None	None
Venezuela	None	None

Source: Compiled from various sources by the editors.

These characterizations of the comparative status of oversight over intelligence services are not definitive, but only indicative of tendencies. Bureaucratic measures can from time to time be taken in any country to accomplish political-military objectives through intelligence capabilities. When a country hosts several intelligence agencies, and when emergency or war-like conditions prevail, the operations of one or another of the agencies may escape direct oversight. For example, although military intelligence remains nominally subject to oversight, intelligence-led operations against terrorist targets abroad, in which even U.S. citizens have been killed, raise the question of whether these actions ordered by the U.S. president as commander in chief should be subject to review or approval by legislative and judicial branches.[195] If the same actions were carried out as a covert action by the Central Intelligence Agency, then congressional intelligence committees would have to be informed beforehand.[196] As further evidence of how oversight provisions shift continually, amendments to the Foreign Intelligence Surveillance Act of 1978, in particular the Patriot Act (Intelligence Reform and Terrorism Prevention Act of 2004), have relaxed the provisions of the 1978 Act, eliminating the requirement that non-U.S. persons be acting on behalf of a foreign power in order to be targeted by U.S. intelligence collectors anywhere within the United States.[197]

Effective intelligence oversight depends on the operation of checks and balances among the legislative, judicial, and executive branches: executive oversight alone is no oversight. Civilian authority over joint military services provides a touchstone for oversight. Where the armed forces remain independent from each other, and not under joint civilian supervision, military primacy in intelligence decisions continues. The pervasive primacy of military intelligence means that only where an intelligence community or intelligence system includes civilian as well as military intelligence services, where system members are not legally free to make their own decisions with respect to intelligence targeting, and legislative oversight is in place, does there exist the possibility of effective oversight over military intelligence. A comparative study of military intelligence oversight in the Americas concludes that military intelligence primacy gives way to civilian oversight only when the armed forces experience a notable failure to accomplish their national mission.[198]

Ethics and Intelligence: Review of European and North American Experience and Its Application in Latin America

Carlos Maldonado Prieto

Introduction

The feasibility of applying ethical principles to intelligence activity poses a question of great importance currently, as well as for the future of professional intelligence practice. Although some pessimists see only contradiction in pairing ethics and intelligence, scholars and intelligence community professionals around the world continually demonstrate the validity of a meaningful connection between the two.

The terrorist attacks of 9/11 in the United States, and the related wars in Iraq and Afghanistan, have revealed an operational intelligence environment where ethical principles have seemed not to apply. The excesses committed by intelligence agents in the "Global War on Terrorism"—whether through the irregular detention of suspects without trial in Guantanamo or Abu Ghraib, through confinement in secret jails abroad, or the torture of suspects by political police in Arab countries allegedly under the auspices of the Central Intelligence Agency—have not only brought on political disapproval but have also raised serious moral questions. Somewhat surprisingly, the strong rejection of these practices by political leaders, academics, and intelligence practitioners themselves has translated into a reexamination of intelligence behavior.

At the same time, in Eastern Europe and Latin America, regions that have been able to overcome the authoritarian political regimes of the waning years of the Cold War, intelligence reform moves ahead. This reform includes drafting and implementing laws to regulate intelligence activity, developing professionalism among intelligence practitioners, introducing legislative and judicial mechanisms of control, and initiating accountability among the intelligence services.

Through an academic discussion of ethics in intelligence and the exploration of some national experiences in intelligence reform, this essay will address the feasibility of an ethical or "deontological" code of behavior in intelligence like

that in other professions such as medicine, law, or engineering. The essay will also comment on appropriate elements of a prospective ethical code.

Conceptual Definitions

Ethics by definition examines the value of conscious human actions freely engaged in; that is, those actions over which the individual exercises some degree of rational control. Ethics not only examines how or why acts are committed; it also seeks to assert a judgment as to whether the acts are good or bad. Ethics asks what actions appear morally correct, how a moral system can be rationally justified, and how it can then be applied to the various aspects of one's social and personal life. In daily life, ethics represents a way to reflect on moral choices and to identify the reasons why a particular moral system may be preferable to its alternatives.[199]

Some observers claim that an ethical proposition reflects the norms espoused by a philosophy or a religion, whereas morality reflects how strongly individuals feel toward the social values of a group. In practice, however, the two concepts remain indistinguishable and equivalent. The nuance that does distinguish one concept from the other appears with practical application. That is, ethical judgments will remain theoretical, while morality arises from the practical application of those judgments. Additionally, morality is based on the values imposed by our conscience, which in turn are based on learned customs or rules. Therefore, morality is neither absolute nor universal, given that its expression depends on the customs in a given region, just as ethics cannot have absolute validity because of its hypothetical basis.

Deontology, the study of morality, refers to the branch of ethics that addresses the foundations of "the ought," or moral norms. Deontology exists to consider the set of moral obligations or duties felt by professionals in particular fields. Deontology is also known as the "theory of the ought."

Professional deontology thus refers to the principles and rules that regulate or guide the conduct of practitioners. These norms determine the minimum behavioral requirements for professionals. Professional bodies generally establish norms for their own field, and codify norms as written rules. The bodies also control in some way the acceptance of new members into the professional ranks, often through a requirement to demonstrate adequate

accomplishment of tasks associated with the profession. Today, practically all professionals have developed their own codes of conduct, including physicians, lawyers, and journalists, among others. To promote and maintain compliance with these "deontological" codes, many professions depend on the existence of professional schools. The norms included in a code of conduct apply to all members of the profession in question. The norms are guidelines whose purpose is to ensure that a particular activity is carried out in a correct, efficient, and suitable manner.

Ethical or moral standards need to be especially solid for professions that operate on behalf of the state, because of the possible repercussions of injudicious viewpoints and actions. This holds true for the military and for law enforcement officials, including police, judges, prosecutors, and similar professionals. By extension, officials of an intelligence community also need to think and behave prudently, given that their profession originated principally from within military organizations. Beginning in the 19th century, ethical standards were introduced in the military profession to humanize warfare, to preserve the life of the wounded and of war prisoners, and to safeguard the physical safety of the noncombatant population. These ethical concepts gained wide applicability through the Geneva Conventions of 1864, 1906, 1929, and 1949. Additionally, in 1948, the United Nations proclaimed the Universal Declaration of Human Rights, which among other things declared the inviolability of civil and political rights for individuals and prohibited torture and degrading treatment.

Intelligence Ethics and the "Global War on Terrorism"

The September 11, 2001 attack on the United States and the subsequent invasion of Iraq on 20 March 2003 have become associated with the apparent failure of the U.S. Intelligence Community to prevent the terrorist acts. Equally, the intelligence services' large-scale violation of ethical principles in the name of President George W. Bush's "Global War on Terrorism" have evoked criticism in many circles. Notably, several U.S. Intelligence Community practitioners and some academicians associated with it have voiced "insider" criticism, allowing us a deeper appreciation of these phenomena.[200]

It is not merely coincidental therefore that 2006 saw the formation of the International Intelligence Ethics Association (IIEA) in Washington, DC. This

organization has held conferences in the United States and United Kingdom, bringing together specialists from the Anglo-Saxon world, Israel, France, India, and other countries. Since 2010, the organization has published the *International Journal of Intelligence Ethics*.[201]

Some studies of intelligence ethics confirm the view that U.S. intelligence professionals have long resisted the idea of subjecting themselves to ethical principles. This stance likely appears among intelligence personnel of all of the countries involved directly or indirectly in the Cold War. An illustrative example comes from Thomas Braden, an ex-CIA agent, who in 1967 published the suggestive article "I'm Glad the CIA Is 'Immoral'." In the view of Allison Shelton, his attitude likely arose from his participation in the contest with the Soviet Union, where any weakness among the participants would have meant defeat.[202] A similar viewpoint comes from federal judge Richard Posner, who recently observed, "Intelligence is the second oldest profession, and the one with fewer morals."[203] According to this style of calculated thinking, which corresponds with the "realist" approach to international relations and "just-war theory," intelligence serves the purpose of supporting national security, with every other consideration subordinated to that end. Shelton notes that, in contrast, the ethical thinking associated with the philosophy of Emmanuel Kant emphasizes moral absolutes.[204]

Shelton also identifies an unsettling paradox in intelligence ethics: Although "it is a fact that most (if not all) intelligence activity has a legal basis in the United States, those activities directly violate or ignore international law and the laws of other countries. My view is that U.S. intelligence activity becomes paradoxical when that country at the same time takes on the role of champion of democracy across the whole world."[205]

Two observers from the United States, Tony Pfaff and Jeffrey Tiel, spot a permanent tension between "ethical moderation" and "intelligence efficacy."[206] At what point may one override ethical principles, and is that decision affected by our being at war? An illustration of this dilemma comes from the issue of officially sanctioned assassination. In peacetime, assassination appears clearly wrong and immoral, whereas in wartime it seems acceptable. The same may be said about the use of deception (an agent using a false identity) or about lying. Both are morally reprehensible, but sometimes justifiable, depending

on operational needs. Other activities, such as inciting illegal actions, bribery, blackmail, and stealing, provide similar examples. The authors conclude that

> because the work of intelligence professionals is indispensable to the national security duties of the state, espionage is itself a derivative moral obligation. This means we should dispense with the idea that somehow the work of the intelligence professional is not compatible with the dictates of morality. But since the road to hell is paved with good intentions and lines do get crossed, it becomes imperative to establish moral boundaries, so intelligence professionals can execute their duties in clear conscience. This is not only good for the professional; it is good for the profession, and given the profession's importance, for the nation as well.[207]

From a different point of view, a well-known Central Intelligence Agency analyst and Soviet Union expert with 24 years of experience,[208] points out that presidents of the United States are guilty of having politicized the agency over the course of three decades. Since the administration of Jimmy Carter, no one has attempted to reform this organization. In this analyst's opinion, four problems have contributed to the downward path of the Intelligence Community: 1) militarization of intelligence that has translated into dependence on the priorities of the Pentagon (Defense Department); 2) a lack of effective congressional oversight; 3) the illegal actions of the CIA's National Clandestine Service, a unit created in 2005 and responsible for paramilitary special operations; and 4) the community's and CIA's mistake of not speaking (inconvenient) truths to the country's political leaders.[209]

Despite the thrust of these suggestions for improvement, Presidents Franklin D. Roosevelt and George W. Bush did engage in efforts to learn and apply lessons from the intelligence failures at Pearl Harbor in 1941 and the Twin Towers of 2001, and Presidents Gerald Ford, Jimmy Carter, and Ronald Reagan prohibited government employees (CIA agents) from engaging in political assassination abroad.

President Ford based his decision prohibiting assassination on the findings of the U.S. Senate's Church Committee. The committee investigated assassination attempts against Fidel Castro of Cuba, Patrice Lumumba of the Congo,

Rafael Trujillo of the Dominican Republic, Ngo Dinh Diem of South Vietnam, and General Rene Schneider of Chile. These episodes occurred during the Eisenhower, Kennedy, and Johnson administrations. The Church Report condemned these abuses: "We consider that [political] assassination violates fundamental moral precepts of our way of life…. We reject absolutely any notion that the United States should justify its actions by the standards of totalitarians."[210]

President Ford signed an executive order that prohibited assassinations. Jimmy Carter did the same in 1978 and Ronald Reagan followed suit with his Executive Order 12333 in 1981, which continues in effect. However, none of the executive orders defines assassination. One can infer that the first executive order in this chain was influenced by the Church Committee Report, which expressly condemned assassination or attempted assassination of foreign political leaders hostile to the United States. Even so, we cannot be certain of the meaning of assassination in the executive orders because none of the three presidents offered public comments explaining their orders.[211]

Politicization of intelligence offers additional examples of ethical dilemmas. Politicization refers to an anomalous relationship between a political leader and intelligence personnel that, in an ideal world, should be professional and apolitical. Discussion of this phenomenon has centered on the political manipulation used to justify and begin the second Gulf War. The supposed possession of weapons of mass destruction by the regime of Saddam Hussein led to the war.

From an insider's perspective, Goodman accused the CIA of allowing politiciziation. He claimed that its most experienced office chiefs and analysts violated all the rules of the analysis process in helping the Bush administration build its case for the invasion of Iraq. "There are filters in the directorates of intelligence and operations to prevent the introduction of fabrications into finished intelligence products, but managers and analysts ran through a series of red lights."[212] This meant that President Bush used erroneous reports of Iraqi purchases of uranium (yellowcake) in Niger to justify his assessment presented in the State of the Union address in 2003. The same type of error occurred with the supposed connection between the Iraqi regime and al-Qaida and the legend about the existence of weapons of mass destruction in Iraq, using the fantasies spread by the Iraqi National Congress.

Widespread Absence of an Ethical Code for Intelligence Practitioners

The politicization of intelligence is not an exclusively U.S. phenomenon. The German observer Erich Schmidt-Eenboom has revealed transgressions carried out by the Foreign Intelligence Service of Germany (BND), illustrating that other mature democracies are not free of illicit practices that compromise professional ethics. He considers that

> the need for the State to put a brake on the autonomy of intelligence agencies is based on a false impression heightened by the sensationalist press, which suggests that intelligence services often act behind the back of the government, pursuing their own ends. In fact, this occurs only in exceptional cases.[213]

He maintains that "supervision of subordinates by intelligence leaders is intentionally laissez-faire by those in the Chancellor's office. In this way, they try to interfere as little as possible in the efficiency of the intelligence services, and tend to look the other way when the services overstep their legal limits."

The same author exhaustively explores infractions, errors, abuses, and illegalities committed by German intelligence. Among the most serious vices discussed:

a. **In the case of intervention in the conflict in what was Yugoslavia:** The BND tried to supply weapons to Croatian forces in 1994, mocking the United Nations arms embargo, and also cooperated with the Kosovar terrorist group UCK;

b. **Spying on and infiltrating legal political parties:** After 2006, the Internal Intelligence Service (BfV) increased the breadth of surveillance of political parties, using intrusive methods. Targets included members of Parliament of the ultra-right (NPD) and the leader of a leftist party, Oskar Lafontaine. This activity occurred in the 1990s when the Green Party was watched and even infiltrated. Schmidt-Eenboom asserts that this activity was initiated on behalf of traditional political parties to maintain the existing party system;

c. **Observation of journalists and scientists:** The nuclear physicist Klaus Traube was illegally targeted for surveillance by the BfV in 1975; the BND intercepted telephone calls of the writer Günther Wallraff in 1976; the BND has continued to target journalists;

d. **Cooperation with regimes that have violated human rights:** In the fight against terrorism, the BND has not hesitated to cooperate with countries—mainly Arabic—that systematically employ torture;[214] and

e. **Cooperation with Nazi war criminals:** Intelligence archives have revealed that Klaus Barbie, the "Butcher of Lyon," in 1966 cooperated with the BND from his refuge in Bolivia. This war criminal wrote 35 reports on political topics—including possibly German arms sales to South American countries—that were paid for by the BND. Further, the BND knew the location of another Nazi criminal, Adolf Eichmann, eight years before Israeli agents kidnapped him in Argentina in 1960.[215]

Emergence of Codes for Ethical Intelligence Practice

The development and acceptance of a code of ethics for intelligence may depend on whether practitioners in an intelligence community consider their business a professional occupation. If they do consider this line of work a profession, then the fact that almost every profession has a code of ethics that imposes certain behavioral limits on professional practice becomes germane to intelligence professionals. Still, some authors believe that intelligence does not need a code of ethics; others believe that it does.

One author who denies the need for an explicit code is Stefan Brem, who works in the Federal Office for Civil Protection in Switzerland, and whose views represent the European model of multiple, external controls on intelligence activity. Brem considers it sufficient to have clear rules and regulations, quality external control, professional accountability, and institutional transparency. He cites five key recommendations contained in the "ten commandants" adopted by the Committee of Ministers of the Council of Europe in July 2002. Compliance with these five recommendations would mean that no intelligence service could be accused of engaging in behavioral excesses or violations of a professional ethic. The five are:

a) **Prohibition on arbitrariness:** respect for human rights, avoiding all forms of discrimination or racist treatment, and appropriate supervision of processes;

b) **Legality of antiterrorist steps:** all the measures need to be legal, and when they impinge on human rights, the measures must be defined precisely and their severity must be in proportion to the desired ends;

c) **Absolute prohibition of torture:** torture and all degrading treatment must be avoided, particularly during the arrest phase;

d) Provisions for the collection and processing of personal information: these procedures need to be covered by internal laws, their depth and breadth must be proportional to the desired ends, and they must be overseen by an independent authority; and finally

e) Measures that interfere with the privacy of persons—such as forced entry for searches, telephone intercepts, the use of undercover agents, and others—need to be addressed by law, with potential review by a judge, and the use of force needs to be proportional to the ends sought.[216]

Still in Germany, Schmidt-Eenboom argues that a code of ethics would reinforce political controls of the intelligence function, thereby reducing or preventing violations of professional ethics. He has suggested the creation of an inspector general for the intelligence services, an office that would act as an institutionalized investigative body in the Office of the Federal Chancellor. The very existence of this institution would have a beneficial effect on the daily activity of the intelligence services by reducing arbitrary, internal punitive measures. A good illustrative example already exists: A parliamentary representative of the Defense Ministry is fully empowered to ensure that the human rights of soldiers are not violated.[217]

The majority of authors consulted, not only from the United States and Germany but from numerous other countries, appear inclined to establish some form of professional ethics code for intelligence agencies. Brian Snow offers an example of a ethics code for intelligence. Snow worked for 34 years as an

analyst for the National Security Agency of the United States. According to Snow, the code should contain at least 11 behavioral standards:

a) First, do no harm to U.S. citizens or their rights under the Constitution;

b) Uphold the constitution and the rule of law; we are constrained by both the spirit and the letter of the laws of the United States;

c) Expediency must never be an excuse for misconduct;

d) We are accountable for our decisions and actions and support accountability processes to ensure our adherence to these principles;

e) Statements we make to our clients, colleagues, overseers, and the U.S. public will be true, and structured not to mislead or unnecessarily conceal in any way;

f) We will seek to resolve difficult ethical choices [in a way favorable to] constitutional requirements, the truth, and our fellow citizens;

g) We will address the potential consequences of our actions in advance, especially the consequences of failure, discovery, and unintended consequences of success;

h) We will not make decisions that impose unnecessary risk on innocent parties;

i) If an action might result in harm to our citizens, we will seek authorization from a national authority external to the agency that is in the chain of command;

j) Although we may work in secrecy, we will behave so that when our efforts become known, our fellow citizens will not be ashamed of us and of our efforts;

k) We will comply with all public and international human rights agreements that our nation has ratified.[218]

In 2010 Spain's National Intelligence Center (CNI) prepared an ethics code for its practitioners.[219] A few months later, the country introduced judicial preview, whereby any act of internal surveillance or internal communications interception required approval by a competent judge. The provision for external control brings Spain's approach into alignment with that of many Western intelligence services.[220] The Spanish ethics code includes a principle forbidding active participation in partisan politics by CNI employees, and imposes severe sanctions against leaking information. The code of ethics appears to have been ready for activation for several years. The delay reflects the considerable resistance among practitioners to its imposition. Spanish intelligence officials expected that the guidelines could reduce the effectiveness of their service.[221]

Some observers believe that an intelligence community should have a professional *ethos*, a more inclusive and profound concept than a list of items in a code of ethics, and a phenomenon that cannot be imposed from outside. According to Albert Pierce, a professor at the National Defense University in Washington, DC, an ethos is concerned more with "who you are" than with "what you do." A professional code of ethics may derive from and be developed from an ethos, but it deals only with what one does. An ethos is organic, in the sense that it needs to develop through a bottom-up, then a top-down bureaucratic process within an intelligence organization. In summary, an ethos needs to grow through introspection within an organization, taking into account its professional functions, its role in national security, and its nature as both a service to the public and to the state.[222]

Ethical Intelligence Reform in Eastern Europe and Latin America

Intelligence reform has remained a key issue in the democratization of formerly socialist countries, and the redemocratization of Latin America. The debate about professional ethics and political-institutional control of intelligence in the United States and Western Europe has contributed to the reform impulse in the new democracies and provided models to emulate or modify. Intelligence reforms established in Eastern Europe and Latin America derive from intelligence ethics discussion cited earlier in this essay.

An Ethical Transformation: Intelligence as Public Service

Following the collapse of the Soviet Union and the reorientation of Eastern European countries, the repressive social control instruments of these one-party states were dismantled. In the case of the intelligence services, these countries had to confront the classical challenge of "democratizing intelligence"[223] by finding a suitable balance between efficiency and transparency and profoundly transforming a function that for decades epitomized anti-democratic practices. Among the transformations: a) a doctrinal change, which recognized that intelligence had now abandoned its primary role in defending the socialist state, and had become a public service susceptible to public scrutiny and external control; b) a behavioral change, involving the establishment of a legal framework respecting laws and avoiding insertion into or interference in political processes; and c) an institutional change, whereby the intelligence community organized itself in a fashion commensurate with the size of the country and its specific needs, with specialized personnel and managers, and operating with confidence and political independence.[224]

Across Eastern Europe, old intelligence agencies disbanded or underwent reform, laws identified specific agency functions, and government committees introduced executive and judicial controls. In Poland, for example, the Committee for Special Services began to oversee the new agencies from its base in the Committee of Ministers. In 1991, the Czech Republic, following the British model, established the Council for the Coordination of Intelligence Services. Hungary, in addition to instituting executive, parliamentary, and judicial controls, installed a public defender and a Commission for the Protection of [private] Information. Slovakia's new Information Service, in existence since 1993, only engages in analysis—and it may not detain individuals.[225]

Public Service Ethos Easily Subverted

Reform of intelligence services typically does not proceed smoothly. Serious problems such as nepotism, corruption, clientelism, and blackmail continued to afflict Eastern European countries even as these countries began to join the European Community.[226] Most of these countries have joined NATO, become part of the European Union, and identify with the Eurozone and the Organization for Security and Cooperation in Europe (OSCE). Additionally, the more developed Eastern countries—Slovakia, Slovenia, Estonia, Hun-

gary, Poland, and the Czech Republic—enjoy membership in the exclusive Organization for Economic Co-operation and Development (OECD).

In Latin America, intelligence services similarly continue to suffer from serious ethical problems and political interference.

> There is evident tension between the function of intelligence and democratic life in these countries. The intelligence services cultivate secrecy, often do not respect citizens' rights, and violate their privacy. These tendencies conspire against the legitimacy that this essential government function should have.[227]

Furthermore, today's political or partisan approach to intelligence merely repeats history. Political clientelism converts intelligence agencies, along with other organs of the state, into booty or plunder for certain factions of political parties or governing coalitions. In extreme cases, the intelligence services, with their history of providing useful political tools (clandestine intercepts, selective espionage, paid informant), become political police in the service of a particular government and against the political opposition.[228]

Creation of New Intelligence Agencies to Institutionalize Behavioral Reforms

The process of intelligence reform has produced advances and reversals in step with the political realities of each country. Some early advances occurred in the Southern Cone and Brazil once the military dictatorships disappeared. In their wake new intelligence agencies emerged in Brazil (Brazilian Intelligence Agency, 1999) and in Chile (Directorate of Public Security and Information and National Intelligence Agency, 1993 and 2004, respectively). In Argentina, reform led to the reinvention of an existing agency. Other episodes of reform have appeared more recently, accompanying the demise of an authoritarian government in Peru in 2001; a security crisis in Ecuador in 2008; corruption scandals and illegal intelligence activity in Colombia beginning in 2005; and a seismic political shift, in the case of Mexico after 2000.

The Colombian case involving the Administrative Department of Security (DAS) stands out as the most dramatic example of intelligence reform. Reform came after a prolonged process of institutional deterioration. DAS

directors, managers, and workers were accused of assassinations, inappropriate arrangements with paramilitary and guerrilla groups, and wiretaps—the famous "chuzadas"—of judges, politicians, and journalists, among several other crimes. A special commission for reform established in 2005 produced no viable change. The DAS, in place since 1953, was then dissolved and replaced by a new organization in 2011. The new agency became known as the National Intelligence Directorate (DNI). According to the director of MI6, the British foreign intelligence service, the new Colombian agency will receive specialized support from British intelligence services.[229]

As Colombian President Juan Manuel Santos tersely noted, "[I]t is sad but true: change in intelligence services arises from crises. And we need to know how to take advantage of crises." The new entity will not involve just a change in name because "this agency will be something completely new, something that has never before existed in this country: a civilian agency dedicated exclusively to intelligence work." He added that the DNI "will not have the authorities of the judicial police," branding as insane the idea that intelligence would engage in detention of individuals, a practice evoking the dark days of the Southern Cone dictatorships. He added that "this agency will work silently for the common good," and pointed out that "we are looking for professionalization through a new professional career in intelligence."[230]

The Colombian Congress in 2011 also approved a new intelligence and counterintelligence law that expressly guarantees respect for human rights. Its article 4 notes that

> the function of intelligence and counterintelligence will be restricted to a strict interpretation of the Constitution, Colombian laws, International Humanitarian Rights and International Human Rights law. In particular, the function of intelligence will be limited by the principle of the rule of law, which guarantees the protection of the right to one's honor, one's good name, personal and family intimacy, and to due process. No intelligence or counterintelligence information may be obtained for reasons other than: a) to ensure the attainment of the essential purposes of the State, the viability of democracy, territorial integrity, sovereignty,

> security and defense of the Nation; b) to protect the democratic institutions of the Republic, as well as the rights of persons resident in Colombia and of Colombian citizens at any time and place—especially the right to life and personal integrity—in the face of threats such as terrorism, organized crime, narcotrafficking, kidnapping, arms trafficking, munitions, explosives or similar material, money laundering, and other similar threats.[231]

Similarly, article 37 declares that the long-standing principle of "due obedience"[232] will not be accepted

> in those cases where the public servant possesses information related to the commission of genocide, extrajudicial killings, torture, forced relocation, forced disappearance, large-scale sexual violations, crimes against humanity, or war crimes committed by a public servant. Public servants in intelligence agencies can report criminal activities of which they have knowledge either directly or through a representative of the intelligence agency, in such a way that their security and integrity is respected, along with the [usual] protection of sources, means, and methods.[233]

Ecuador provides a second case worthy of analysis. Although in this country there did not exist the massive political repression that characterized the Southern Cone and Brazil, excesses nevertheless did occur in the 1980s. A Truth Commission investigated the violations of human rights committed from 1984 to 2008 by members of the armed forces, national police, and other agencies of the state related to the area of national defense and internal security, including intelligence agencies. The commission verified a total of 456 victims, the majority of them aggrieved between 1984 and 1988, the period coinciding with the presidency of Leon Febres Cordero and with the period of maximum activity by the guerrilla group *Alfaro Vive Carajo*![234]

As a result of the 2008 Colombian attack against the FARC camp situated in Ecuadorian territory, an official commission was set up to explore the facts behind the episode. Among its findings:

> The lack of prompt action by the Ecuadorian intelligence agencies to notify the country's political leaders, the serious nature of the events on national territory, and the evidently keen knowledge of the events by Colombian intelligence, brought the highest levels of the Ecuadorian government to decide that there existed an intentional withholding of information orchestrated by foreign intelligence agencies.[235]

As a consequence of this crisis the government dissolved the National Intelligence Directorate and replaced it with the National Intelligence Secretariat (SENAIN) in 2009. However, its slow and weak institutional development warranted criticism—it did not detect beforehand the police rebellion that shook the country in September 2010—and it has had a high turnover of directors, who have alternately been civilians, then military retirees, and vice-versa.[236]

International Promotion of a Professional Intelligence Ethos

In the peculiar case of Chile, with democracy in full bloom in 1993, the navy confiscated all copies of a book written by Humberto Palamara, a retired navy officer, and put him on trial. This exemplified the difficulties encountered in the transition to democracy. The author in question sought the protection of the Inter-American Court of Human Rights.[237] That court in 2006 ruled that Chile had violated Palamara's rights by having applied prior restraint, having violated the guarantee of due process upon illegitimately subjecting Palamara to military jurisdiction, and having violated the right to private property by denying him the use and enjoyment of his intellectual creation. Beyond paying compensation and allowing the publication of the confiscated book, Chile had to bring its military justice up to international standards. Military justice now must limit itself to those crimes committed by military personnel on active duty, and ensure that no civilian be subjected to the jurisdiction of military tribunals.

In his book, finally published in 2006—in compliance with the court's ruling—Palamara severely criticizes the military's violations of human rights, including the use of military intelligence services in antisubversive warfare, and asserts the need for certain ethical boundaries:

> It seems to me that so long as [military] intelligence lacks a code of ethical conduct to guide the actions of individuals

> who work in this field, it will remain vulnerable to satisfying the special interests of corrupt leaders, and it will thus be held back from achieving the prestige of becoming a profession. Until this situation changes, intelligence should be considered simply an activity or an occupation that brings together specialists in the different roles needed to carry out intelligence.[238]

Far more than one individual among the many practitioners of intelligence need to adopt an admirable ethical stance. An enduring expression of moral and ethical responsibilities depends on the power of collective opinion expressed in a multilateral or international convention. In this precedent-setting case, Chile has shown a commitment to accepting the decision of a multilateral legal body in the Palamara case, which may signal a further evolution of intelligence ethics.

Conclusion

This brief review of crimes or excesses committed by some intelligence services suggests three categories that account for the diversity of these phenomena:

a) **Individual:** This category includes robbery, espionage, sale of sensitive material, and extortion for cash. Such individual acts may respond to disciplinary steps taken by security offices, such as internal affairs offices, or by the judicial system;

b) **Institutional:** These include acts committed by the intelligence services as a product of excessive jealousy, autonomy, and corporatism, generally in an effort to gain greater recognition, to gain the upper hand in bureaucratic competition with other agencies, or even as a result of opposition to the approach being taken by the political authority. These, by definition, take place without the consent of the political authority, although it often remains difficult to determine whether that authority has knowledge of the institutional excesses; and

c) **Political:** These amount to a type of institutional excess, distinguished by being ordered by politicial authorities. They may include fabrication of evidence and generally involve the

persecution of opposing politicians, journalists, judges, or other politically irritating individuals or organizations.

Combatting the crimes or excesses in the last two categories requires methods distinct from those used against individual acts. The three types of crimes or infractions described here occur commonly around the world. In effect, no country is free of these afflictions. Differences do exist from place to place in the level of impunity allowed, however.

Even with the full implementation of ethical precepts and their acceptance by intelligence personnel, there will likely always remain areas of behavior not subject to control. When a political authority orders or consents to excesses, for example, control becomes less feasible. The possibility for control seems remote in cases of political persecution or spying on bothersome individuals or organizations within the country, whether opposing politicians, journalists, judges, or environmental leaders. These excesses call for the invention of mechanisms to avoid their occurrence.

This essay asked whether ethical violations and behavioral excesses require a professional code of ethics for intelligence organizations, or whether a powerful system of external control might suffice. An optimal solution would employ both approaches. Intelligence services could develop or adopt professional ethical standards like those described in this essay, and they could apply recommendations for acceptable behavior that come from external, international organizations such as the Council of Europe or the Organization of American States (OAS).

Additionally, a professional *ethos* would add a highly personal element for an intelligence service to define "who we are." An ethos should emerge organically from within intelligence organizations, thereby demonstrating its centrality to professional practice. Once incorporated into intelligence practice, an introspective ethos may reinforce professional development by ensuring fair, merit-based selection of personnel; establishing a career path from entry until retirement; maintaining career incentives and support of continuous professional improvement; and establishing precise and rigorous rules for performing the various jobs available during all stages of an individual's career.

There exists no universal code of ethics for intelligence, nor anything even approaching such a universal code. The Spanish example discussed earlier demonstrates one of the main reasons why this is the case: The imposition of an ethics code awakens natural resistance from within the intelligence services. However, a code offers clear benefits to intelligence services through its ability to improve the image of intelligence in public opinion. The challenge of creating a code of ethics for intelligence requires patience, common sense, and persuasive argument.

Legislators and politicians can intervene to promote the development of a code of ethics. Legislators have thus far generally avoided involvement in intelligence matters, but in this instance, they could couch their involvement in terms of the protection of human rights and personal privacy. Legislation oriented toward the control of the intelligence services should include penalties to deter those who might commit crimes and excesses by disregarding widely acknowledged professional ethical standards.

Politicians also bear some responsibility to influence ethical behavior among the state's intelligence personnel. Every intelligence service, whether operating inside a country or abroad, should be able to count on the example and guidance of the leader of the executive branch. A political leader should protect the intelligence services, giving them clear and limited missions to promote efficiency. At the same time, the leader needs to prevent unacceptable behavior by identifying clear guidelines that cannot be ignored or crossed. With this guidance, the intelligence services will not have to face the difficult task of deciding for themselves how far they can go to fulfill their mission on behalf of political leaders. If the political leader manipulates the work of intelligence agencies for his or her own ends, which can be at odds with the well-being of the state and of the society, then the remedy for this tendency lies with the electorate.

Politicians also bear the responsibility of appointing capable leaders of the intelligence services and identifying their expectations of the appointee. It is not enough that intelligence chiefs demonstrate expertise in security, diplomacy, terrorism, and similar topics; they must also have impeccable moral standards and unreproachable character. Their leadership of intelligence

organizations will establish de facto standards for the professional activity of their subordinates.

Where a truly empowered civil society stands guard against threats to citizen rights, the independent press and other organizations have an obligation to scrutinize politicians and intelligence services. Intelligence-related crises that have ended in reforms or new legislation have usually come to public attention through accusations by journalists and other social activists.

The intelligence services themselves can improve their image by complying with one of the greatest concerns of contemporary society—that intelligence personnel act responsibly and periodically engage in transparency. The English-speaking world knows this as "accountability." A variety of options exists to demonstrate accountability, from delivering an annual report on activities and budgetary details to congress, to broadcasting intelligence intentions (its ethos) to the public through web pages or other means of dissemination.

Ethics contributes to the daily work of intelligence agencies around the world. Every aspect of intelligence, whether analysis or operations, benefits from observing solid ethical principles. In some agencies, intelligence ethics codes will appear; in others, ethical guidelines will suffice. Either approach will lead this government function, whose work always raises questions, along the path to respectability and legitimacy.

Author's Biography

Chilean **Carlos Maldonado Prieto** holds a degree in history from Martin-Luther-Universität, Halle, Germany. He also earned a master's in defense policy from the Chilean Army War College. In the United States, he has served as an academic fellow at the Western Hemisphere Institute for Security and Cooperation (WHINSEC) and has participated in courses and seminars organized by the Center for Hemispheric Defense Studies (CHDS). Maldonado's publications include *El Prusianismo en las Fuerzas Armadas Chilenas: Un estudio histórico, 1885–1945* (Santiago: Documentas, 1988) and *La Milicia Republicana: Historia de un Ejército Civil en Chile, 1932–1936* (Santiago: Servicio Universitario Mundial, 1988). He has also published articles on intelligence, the history of the armed forces, military service, and police issues in German, Canadian, Chilean, U.S., Japanese, Peruvian, and Swiss journals. **Email:** *cmaldona99@gmail.com*.

Human Rights and Intelligence Ethics: Case Studies from Cinema

Moira Nakousi Salas
and
Daniel Soto Muñoz

Intelligence and the Rule of Law

The rule of law in Latin America dates to the region's 19th-century national independence movements. The new republics adopted a liberal European philosophy with limits to the exercise of government power. Although the anthropomorphic state retained the undisputed sovereign right to make decisions and issue mandates within national territory,[239] it accepted limits to its own actions. The main limit to its power came from honoring the concept of individual human rights.[240]

The executive branch remained responsible for public well-being and for carrying out functions basic to the survival of the collective society. The state's former focus on legitimizing the use of force against citizens gave way to greater governmental concern for citizens. The use of force has, since independence, been the last resort of governments to ensure citizen compliance with laws. Government now uses force to guarantee public security in the face of internal and external threats.[241]

From the beginnings of the modern state, the main concern of governments has been the exercise of sovereignty, and in particular, maintaining a balance between security and freedom. For most of the 20th century, the concept of security exclusively meant state security. Systematic violations of human rights were justified as unfortunate but unavoidable to ensure the security of the state. By the end of the 1990s, concepts of "human security" and "multidimensional security" emerged, changing the security focus to individuals.[242]

The film *Unthinkable or El día del juicio final*, the central focus of this study, offers a raw portrait of issues in public security policy. In a democracy, the need to prevent or repress a threat conflicts with the social costs of restricting

individual rights and freedoms.[243] The extreme scenario asks whether official actions that might benefit an entire community, but that take away the most basic rights of some individuals, can be justified. The film's director places the viewer on the side of innocent victims. This perspective avoids the dilemma facing intelligence: how to guarantee the security of residents without severely restricting freedoms.[244] This essay will go beyond the approach used in the film by exploring the unavoidable choices facing intelligence professionals operating under the rule of law.

A focus on the rule of law by security forces helps ensure public well-being but may put an individual's right to life and freedom of action at risk. In an alternative view, security serves as a tool to guarantee the more important, individual human rights.[245] Every political regime develops its own interpretation of these views, and applies them to its intelligence agencies. Whereas in democratic regimes, intelligence exists precisely to affirm individual freedoms, in totalitarian regimes, security becomes an ideology that places intelligence agencies at the service of powerful interests bent on restricting individual human freedom.

Additionally, under the rule of law, all institutions, including the intelligence agencies, face restrictions. Intelligence exists to prevent the development of threats to security. It does not have a deliberative role in the conduct of the state. However, in ideological (totalitarian) regimes, in bureaucratic dictatorships, and at times even under democratic governments, the discovery and punishment of "internal enemies" becomes a priority.[246] In any of the three regime types, intelligence services may reflect this urge to repress potential dissidents.[247] Intelligence services have an opportunity to dispense with this internal security role by shifting their allegiance to democratic norms.

The film industry offers interesting examples of these three models of government and their respective public security faces. *The Lives of Others* (*Das Leben der Anderen*) explores the implacable and persistent violation of the right to privacy, including intimacy, in East Germany. The political police, the *Stasi*, used this invasive tactic against dissidents who opposed the communist regime of the German Democratic Republic.[248] The Argentine film *The Secret in Their Eyes* (*El secreto de sus ojos*) deals with the impunity enjoyed by a common criminal who worked for a security agency during the years of military rule.[249] *Burn After Reading* follows the traumatic retirement of Osborne Cox,

forced to end a long career as an intelligence analyst in the United States.[250] (See Table 4.)

Table 4
Typology of Forms of Government and Their Intelligence Agencies

Government Type	Agency Type	Film
Totalitarianism	Political police	*The Lives of Others* by F. von Donnersmarck (2006)
Authoritarianism	Independent security agency	*The Secret in Their Eyes* by J. J. Campanella (2009)
Rule of Law	Intelligence system	*Burn After Reading* by the Coen brothers (2008)

Source: Developed by the authors, following Gonzalez, Larriba, and Fernandez, "Servicios de Inteligencia y Estado de Derecho," in Jose Luis Gonzalez Cussac, coord., *Inteligencia* (Valencia, Tirant Lo Blanch, 2012), pp. 284–287.

Setting the Stage: The Film *Unthinkable*

The scene: A detainee admits to having planted three nuclear devices in different urban centers across the country. In a video, the individual declared that the three bombs will go off simultaneously four days from now. Authorities have learned that the devices could cause between six and ten million deaths. The detainee refuses to volunteer information that would allow deactivation of the devices, or the evacuation of potential victims. Under the rule of law, is it legal and moral to consider torturing this individual to save the lives of millions of residents? This is the dilemma posed in the 2009 Gregor Jordan film *Unthinkable* (Spanish-language title *El día del juicio final*), and the central question for intelligence professionals to consider.[251]

Intelligence and Human Rights

In this scenario, television broadcasts are reporting on the search for a fugitive accused of assassinating a policeman and kidnapping two children. Authorities release his photo and ask the public to help find him. The counterterrorism unit of the Federal Bureau of Investigation (FBI) in Los Angeles begins

its own investigation, but for a different purpose than that presented to the public. Special agent Helen Brody receives an order to investigate one hundred possible suspects linked to the fugitive. The order is from headquarters. She has support from the FBI and local police to find and detain these persons. The suspects all have ties to radical Islamist terrorist cells operating in the United States.

Intelligence services normally have authorization to take actions that may restrict individual rights and freedoms. Intelligence laws typically allow agencies to monitor persons of interest, intercept personal communications, and employ undercover agents and informants. Intelligence services with police powers can also enter and search private spaces, can search individual persons, vehicles, and luggage and can detain and arrest individuals who pose a threat.

The rule of law stipulates that these actions be taken only on an exceptional basis, under certain circumstances, and always subject to oversight and control by executive, legislative, or judicial officials. Therefore, these special procedures are usually carried out by police forces under judicial supervision. Not unlike intelligence personnel, police officials generally refrain from disclosing actions taken and releasing information so obtained.

Latin American intelligence systems operate under laws that explicitly acknowledge the need to preserve constitutional order. These laws oblige intelligence agencies to use information-collection methods that comply with constitutional requirements. The laws also include language obligating intelligence officials to respect individual human rights. (See Table 5.)

Table 5
References to Human Rights in Latin American Intelligence Laws

Country	Intelligence Law	Articles	Date of Constitution	Relevant Constitutional Sections
Argentina	25520 of 2001	3, 4, and 5	1994	8, 14, 15, 18, 20, 33, 75 No. 22, 23, 24, 86
Brazil	9883 of 1999	1.1	1998	1, 4.II, 5.XLI, LXXVII.1, 17
Chile	19974 of 2004	3, 4 and 34.c	1980	1, 5 section 2, 19.

Table 5
References to Human Rights in Latin American Intelligence Laws (continued)

Country	Intelligence Law	Articles	Date of Constitution	Relevant Constitutional Sections
Colombia	195 of 2011	2, 4, 14, 15, and 24	1991	11–41, 91–95, 118, 164, 214, 222, 277, 282
Ecuador	Official Law Registry No. 35 of 2009	4, 19, 23, 30, and 33	2008	10, 11, 18, 27, 41, 51, 57, 58, 66, 83, 93, 156, 158, 163, 171, 384, 398, 416, 417, 423, 424, 426, 428, 436
Mexico	National Security Law of 2005	25 and 31	1917	2.A.II, 2.B.VIII, 21, 102.B
Peru	28664 of 2005	3 and 4	1993	1–3, 14, 44
Venezuela	Official Gazette 38940 of 2008	10 and 24	1999	1-3, 19–31, 46, 55, 76, 132, 152, 261, 271, 272, 278, 280, 281, 326, 337, 339, 350

Source: Compiled by the authors.

To avert conflict between the interests of the state and of individuals, intrusive actions by intelligence services must meet tests of legitimacy posed by domestic and international human rights law. International norms that guide intelligence and counterintelligence activities also regulate police investigations.[252] The following cinematic examples illustrate the application of the norms in five contexts. Table 6 will highlight the tensions between special collection activities and international human rights law at play in each of the five areas.

Surveillance and Lookouts

Surveillance (*seguimiento*) includes physical or technical maneuvers that allow the agent to maintain a previously selected target under continuous observation, whether in person or by remote means. A lookout (*vigilancia*) observes activity at a given location.

When a target operates in public spaces, and is not aware of being observed, that individual's rights suffer no apparent curtailment. However, the possibility that the state might save the information obtained does affect an

individual's legal rights. The degree of the effect increases if the state targets private or intimate life. In that case the state may be overstepping the bounds of "predictability."

Uninterrupted state observation of daily activity may create in the target a sense of having restricted freedom of movement[253] or limits on the right of association.[254] Continuous observation can even affect the presumption of innocence by altering the burden of proof with respect to eventual criminal charges.[255]

The film *The French Connection* features extended surveillance by the policeman Jimmy "Popeye" Doyle, who targets all those who may be "connected" with the French smuggler Alain Charnier. The surveillance employs a variety of techniques, with varying results, and extends across much of New York City in the course of targeting and uncovering criminal participation.[256]

Intrusive Measures Targeting Communications

Disruption or interception of communications can involve capturing mail in the postal service system, wiretapping, or systematic monitoring of communications media with remote recording.

These intrusive measures raise the possibility of arbitrary state involvement in the privacy and intimacy of individuals. A citizen's right to privacy and intimacy implies the obligation of the state to be aware of the inviolability of the home, family communications and relationships, and the right of individuals to develop their personality.[257]

The international "Code of Conduct for Officials Responsible for Law Enforcement" addresses the right to privacy.[258] The code's article 4 declares that "information of a confidential nature that law enforcement officials possess will be kept secret until their duties or judicial needs require otherwise." The code applies equally to intelligence officials.

In *The Lives of Others*, a corrupt minister of the German Democratic Republic insists that the *Stasi* acquire and record all private communications, including those of an intimate nature, inside of the home of a dissident playwright. Minister Hempf's motivations are not purely political and the *Stasi's* intense monitoring of communications between Georg Dreyman and his girlfriend greatly affect their public and private life.

Undercover Agents, Infiltrators, and Informants

Undercover agents hide their official identity to obtain information for intelligence purposes. When they make their way into criminal or terrorist organizations, they become *infiltrated* agents. *Informants* do not belong to the intelligence services and supply useful information, usually in exchange for money.

These three types (undercover agents, infiltrators, and informants) present some legal problems for intelligence services because of their secret identities. Secrecy complicates any process for determining source validity in the course of proving that crimes have been committed. This hinders the prosecution as well as the defense. Defenders of the accused, for example, cannot depose anonymous witnesses. Thus, secrecy compromises legal due process.[259]

The use of informants also presents some ethical problems. Informants often have a link to criminal activity, and are motivated to gain protection from the state. In addition, any contact they have with officials remains secret. Informants bring some risk to the security and justice system because they may use their criminal ties to commit crimes with impunity, or they may encourage others to commit crimes using the same information they share with officials. Additionally, secrecy and payments for information can incentivize official corruption.[260]

The Departed does not depict the world of intelligence services, but it presents situations related to undercover agents, infiltrators, and—unexpectedly—informants. The policeman William "Billy" Costigan Jr. infiltrates the criminal organization of Francis "Frank" Costello. At the same time that he works to unveil the structure and operations of this mafia organization, he has to identify a "mole" who has maneuvered his way into the police Special Investigations Unit.[261]

Entering and Searching Locked Premises and Physical Searching of Persons

Police gather intelligence by entering and searching locked premises, also known as "house search" or "domicile search." A house search occurs when the homeowner has not voluntarily consented to a search of the premises, and it constitutes a clear violation of the principle of home sanctity.[262] Sanctity of

the home guarantees due process because it allows a resident to ward off the illegal collection of incriminating evidence.[263]

The physical search of persons, vehicles, or luggage, also called "requisition," targets an individual to find objects and information useful for a criminal investigation. The individual rights and freedoms at play in this case are the same as for searching locked premises. The sex of the agent doing a body search must be the same as that of the individual being searched[264] and should be done in a private setting to maximize the dignity and decorum of the person being searched.[265]

The Green Zone[266] views intelligence from the perspective of armed conflict. It focuses on the difficulties of taking individual rights into account in an occupied zone. The film illustrates how intelligence can influence the design and implementation of military and police operations. In the storyline, military personnel carry out most of the special procedures for collecting information. The film reveals that successful collection of information depends on having clear judicial rules for applying or withholding force during an intelligence operation. An officer faces the always-difficult field determination of whether "law enforcement" (human rights) rules apply to a situation, rather than the less specific rules of international humanitarian law (conduct of hostilities).

Deprivation of Liberty

Government authorities can choose any of various legal paths to deprive detainees of their liberty. They may detain a suspect for a flagrant crime (generally known as "arrest"); they may detain by judicial order or at the request of an administrative official; and they may confine a suspect after sentencing. They may also "institutionalize" a person for health reasons, or "intern" them for precautionary reasons related to public safety. Deprivation of personal liberty can be carried out in public or private establishments, and a principal characteristic is that the detainee loses freedom of movement.

All the reasons for deprivation of individual liberty, including those applied by police intelligence officers, must take into account the subject's right to personal integrity and humane treatment.[267] The most important guarantees ensure that the subject, immediately after apprehension, knows the reasons for his or her detention, appears before a judge without delay, and has a

judgment rendered in the case within a reasonable period.[268] During the entire length of detention, the subject must be treated humanely, with the dignity due any human being.[269] These principles demand that the detainee not be subjected to "legitimate" physical or moral torture, or be exposed to inhuman or degrading interrogation techniques.

The most serious challenge to safeguarding human rights comes with the application of "preventive" detention. Preventive detention brings to mind the abusive interrogation of suspects thought to have terrorist associations. *The Battle of Algiers*[270] recreates counterintelligence operations carried out by France in the Algerian War of Independence. Colonel Mathieu begins to restrict the residents' liberty of movement, and later carries out random detentions and employs brutal interrogation techniques. The purpose of these actions is to find out who may be leading the National Liberation Front.

Table 6
Sources of Tension between Intelligence Activity and Human Rights Protection Exemplified in Selected Films

Intelligence Activity	Judicial Controversy	Norms in Conflict	Film Examples
Surveillance and Lookouts	Presumption of innocence	Universal Declaration (art.11), International Covenant for Civil and Political Rights (ICCPR) (art.14), American Convention (art.8)	*The French Connection* by W. Friedkin (1971)
Intrusive Measures in Communications	Right to privacy, honor, and dignity	Intrusive Measures in Communications Universal Declaration (art.12), American Convention (art.11)	*The Lives of Others* by F. von Donnersmarck (2006)
Undercover Agents, Infiltrators, and Informants	Right to depose witnesses	Universal Declaration (art.10), ICCPR (art.14), American Convention (art.8)	*The Departed* by M. Scorsese (2006)

Table 6
Sources of Tension between Intelligence Activity and Human Rights Protection Exemplified in Selected Films (continued)

Intelligence Activity	Judicial Controversy	Norms in Conflict	Film Examples
Entering and Searching Locked Premises and Physical Search of Persons	Right to personal security and freedom	Universal Declaration (arts. 3 and 11.2), ICCPR (art.9, 11, 14, and 15), American Convention (arts. 5, 7, 9, and 10)	*The Green Zone* by P. Greengrass (2010)
Deprivation of Liberty	Personal integrity and humane treatment	Universal Declaration (art.5), ICCPR (art.5), American Convention (art.5), Convention against Torture, Body of Principles for the Protection of Detained or Imprisoned Persons	*The Battle of Algiers* by G. Pontecorvo (1966)

Source: Compiled by the authors.

Weighing the Actions of Officials in Unthinkable

Whether actions taken by officials in *Unthinkable* conform with international standards of behavior cannot be answered definitively. The film does not pause to consider the judicial implications of the inhumane treatment of the terrorist bombing suspect. It does prompt viewers to consider the real-life implications of security officers' decisionmaking in future national emergencies. For example:

a) At the beginning of the film, FBI Special Agent Phillips shows Special Agent Brody a dossier accidentally sent from the CIA to the FBI. It contains a photo of Humphries (a person of interest at that point) obtained by illegal CIA surveillance. The CIA does not have the authority to collect information on U.S. citizens; it may only obtain information related to foreign intelligence and counterintelligence.[271]

b) Later, Phillips and a colleague break into Humphries's house, without judicial authorization. When they need help, two other agents come to their rescue, detain Humphries, and search the house.

c) The FBI declares that it has information about individuals who may have links to domestic terrorist activities. The legal limits to using the data set remain unknown. The mission appears clear: "We need to interrogate their families, their friends, their colleagues at work, every potential terrorist link in their life over the past nine months, and we need to do it now!" In reality, such large-scale detentions would stand out as arbitrary and illegal.

d) Authorities detain the presumed terrorist, Younger-Yusuf, and keep him at a secret location. He has not yet been told the legal reason for his detention. Originally detained for having a "suspicious attitude," the interrogators seek his self-incrimination. Younger-Yusuf's captors apparently have no intention to bring him before a judge within a reasonable time frame. Officials orchestrating his detention have failed to comply even minimally with international obligations for handling detainees.

Intelligence and Torture

The scene: Authorities have detained Steven Arthur Younger, alias Yusuf Atta Mohamed, for 24 hours. He had surrendered to local police, and confirmed having planted three nuclear devices. No one saw him planting the devices, and no one knows their location. Counterintelligence has confirmed he participated in the theft of radioactive material some years before, and that he knows how to deactivate bombs, including nuclear arms. The armed forces have control of this emergency situation as part of their responsibility to "suppress any insurrection, illicit association, or conspiracy." Until this moment, Younger-Yusuf has been treated appropriately: no beating, but some exposure to heat, cold, sleep deprivation, noise, bright lights, and threats of violence. A government representative instructs Henry Harold Humphries, alias "H," to inflict increasing pain on Younger, with the intention of gaining the information that may save the lives of millions.

By definition, torture inflicts serious physical or psychological pain and suffering on a subject.[272] Modern thought objects to the practice, while

international law and all penal codes forbid its use.[273] Nonetheless, if violating the rights of a few individuals may benefit society as a whole, moral and judicial restraint may not prevail. *Unthinkable* casts restraint aside in dramatizing a "ticking time-bomb" scenario.[274]

Certain factual assumptions support the use of torture in this scenario: an explosive device set to detonate automatically at an unknown location; likelihood of numerous victims; detained suspect declines to cooperate. These assumptions taken together may justify torture to obtain information. Some proponents of torture recommend judicial regulation to avoid its indiscriminate use.

Each of these assumptions, however, appears readily refutable.

First, only if someone has seen the suspect plant the bombs do we know for sure they exist. In that case, the locations would be known. The detainee has incriminated himself, has given information about his activities in a video, and has maintained silence during the first few days of detention. This series of events never occurs in real life. If police were to accept such claims at face value, they would detain dozens of people each day. After torturing perhaps hundreds of suspects, officials might find an explosive.

A second objection arises from the idea that no known torture technique allows one to inflict increasing levels of pain or humiliation. Violence against an individual that meets the definition of torture has dangerous effects on those subjected to it, on those who inflict it, and on those who witness it, no matter its "intensity."

The expectation that a torture victim will reveal accurate information with the infliction of just enough pain further undermines the validity of the film's scenario. A sense of urgency generally accompanies depictions of torture. *Unthinkable* differs from the normal bomb scenario in devoting four long days to mistreating the suspect: asphyxiation with a plastic bag, castration, beating with a cane, prolonged sessions of hanging, electric shock, fingernail pulling, brass knuckles, irritants sprayed into the ears, tooth extraction without anesthesia, long-duration immersion in water, forced observation of a homicide, and the threat of the same against the detainee's children. Viewers see these disturbing episodes while listening to Beethoven's sonata for piano Opus 13

(*Sonata Pathétique*), interrupted by Helen Brody's more humane treatment of Younger-Yusuf.

Intelligence does employ interrogation to elicit information, but not in a ticking time-bomb scenario. In accord with human rights principles, the rule of law typically leads to the designation of torture as a crime. The barbarity of torture as an intelligence tool fits only the corrupt institutions of dictatorial political systems. A Chilean author whose work[275] created controversy has claimed that "a dirty war is not doctrinally part of the activities that intelligence is supposed to perform."[276] He adds that the institutionalization of torture became one of the characteristics of the Chilean dirty war. This disrespect for the life and dignity of individual citizens deligitimized the prevailing "national security" doctrine. He also points out that torture, no matter the method used, always occurs without ethical justification, and that evident respect for life and human dignity "distinguish a criminal from an honorable person." Palamara's simple reasoning appears conclusive.

Intelligence Management

The scene: Younger-Yusuf's actions create a general sense of mistrust, vulnerability and defenselessness among his captors. The state's intelligence system has proved incompetent, the FBI's specialized team unable to connect the detainee with terrorist groups operating inside the country. Additionally, neither the CIA nor other agencies of the intelligence community have detected that a former military man who left the service harboring profound resentment has joined forces with hostile intelligence agencies. Amid these failures and uncertainties, it falls to Harold Humphries, alias "H," to use torture to confirm the existence of the bombs, and to learn where they have been planted.

Unique Identities

The origin of human torture remains unknown. Who first made the cold-blooded and calculated decision to inflict inhuman pain on another person? How can groups of people, organizations, and state apparatuses institutionalize so abominable a practice? What allows the person who inflicts the pain to minimize its importance?

Violence has claimed millions of victims throughout the history of warfare and interpersonal aggression. Political, religious, ethnic, or gender differences

explain much of the violence. But in other cases the explanation rests simply on hate generated by "enemies"[277] who see themselves as common, decent individuals.

Humans naturally and automatically categorize things. Assigning things to categories facilitates the process of understanding complexity in received information. The process allows one's mind to adapt to an environment conceptually and behaviorally. Even young children make choices and put objects, situations, or persons into categories. The eagerness to place things into groups, which emphasizes the common attributes of a set, also highlights the differences among groups.

Social categorization also tends to exaggerate one's differences *vis-à-vis* the individuals placed in other groups. At the same time, we minimize the differences in our own group. We thus arrive at "endogroups" (us) and "exogroups" (them). Within the endogroup, spontaneous attraction predisposes us positively toward fellow members through a process called "gratuitous discrimination."[278]

In the first moments of *Unthinkable*, the antagonist records the video in which he reveals the existence of the nuclear devices. He appears as a "regular guy," although a little nervous. We learn his true identity, revealed by his Arabic name, as he begins to describe his twisted scheme. From that point onward, this young and disturbed man leaves our endogroup, converted into a threat.

Being in a group or being aware of one's social category reinforces "the emotional and values-oriented significance of belonging."[279] Feelings of warmth, strength, protection, and pride arise and generate a new resource—social capital. Building social capital engenders solidarity, militancy, and consistency in the group.[280]

The loyalty and favoritism of the endogroup do not oblige members to express hostility toward the exogroup. Hostility does emerge when a threat (real or imagined) arises to confront the group's identity. In the view of his captors, Younger-Yusuf represents a clear threat because he has already shown himself capable of killing. More than 50 people died in a mall bombing attributed to him. Younger-Yusuf presents himself as a potential martyr, persecuted and

threatened with death by the government.[281] To the detainee, governmental authority continuously threatens the Islamic world.

Government intelligence agents in *Unthinkable* operate in small, strongly indoctrinated and well-equipped teams. They all proudly and prominently display corporate identification badges and accessories—Helen Brody has to rearrange her clothing to hide her firearm as she crosses a street. Military officials show off deep procedural knowledge and their efficiency in executing orders from superiors. The film's dialog reinforces the participants' sense of belonging to separate endogroups.

The illusion of a unique identity or "singular affiliation," easily cultivated and only weakly suppressed, can become a powerful incentive to inflict violence on another group, and it is the point of departure for persecution, torture or extermination.[282] The concept of an enemy emerges from the mistrust of or threats made toward the exogroup. An enemy emerges, whether real, imagined, or intentionally introduced.[283] A sininster enemy justifies any actions to thwart him, and at the same time reinforces one's own identity (See Table 7.)

Table 7
Ideas That Nurture the Concept of Unique Identities

Causes	Type of Singular Affiliation
Superiority of the Endogroup	Ethnocentrism. Chosen group, privileged by nature, or called to a sublime mission.
Feeling of Injustice	Belief in the existence of unacceptable outrages and humiliations that affect the group's territory, rights, and freedoms.
Vulnerability	Real or perceived vulnerability to the other group.
Mistrust	Only bad things can be expected from the other group. This may be collective paranoia or a real history of grievances.
Mistrust	Only bad things can be expected from the other group. This may be collective paranoia or a real history of grievances.

Table 7 Ideas That Nurture the Concept of Unique Identities (continued)	
Causes	**Type of Singular Affiliation**
Defenselessness	Collective perception of loss of control, dependence, and helplessness that lead to insurgency and confrontation.
Goals and Objectives	The greatness for which the endogroup is destined justifies any means toward that end.

Source: Compiled by the authors and based on Amalio Blanco Abarca, "La Condición de 'Enemigo': El Ocaso de la Inocencia," in Manuel Cancio Melia and Laura Pozuelo Perez, coords., *Política criminal en vanguardia: Inmigración clandestina, terrorismo, criminalidad organizada* (Navarra, Spain: Editorial Aranzadi SA, 2008), pp. 296 and 297.

To his captors, Younger-Yusuf belongs in a suspicious category: born in the United States, he grew up in Islamabad and speaks Farsi and Arabic. Although a U.S. citizen, he belongs to another group, the same group as those whose photos appear in the FBI list of terrorism-related suspects. His photo appears next to those of Arabic suspects in the "wanted list." Torturing this suspect becomes a state-supported action. His captors ignore the detainee's nationality, thus depriving him of his basis for a personal identity. Brody tries to argue against torturing this citizen turned "illegal combatant," but a senior authority overrides her argument: "That's who he was yesterday, but today he has no country."

From Misgivings to Inhumanity

Given appropriate social conditions, decent, ordinary people can be led to carry out extraordinary cruelties.

—Albert Bandura[284]

The most brutal personalities in *Unthinkable* live routine lives. "H" for example, a good husband and father, inflicts great pain and suffering on a captive subject. Special agent Brody confronts Rina, H's wife, and reproaches her for living with such a man. Rina replies, "Normal? Let me tell you something. I lost my first family in Bosnia. Three men came into my house. They violated me in front of my family and then they killed everyone in the family. They killed my youngest child last. These were my neighbors. They knew me. They were very normal men." Rina is beautiful and gracious, but fragile because of the unthinkable events in her past. H asks Brody, "Did she tell you the rest of the story? What happened when her town was retaken and they captured these three men? She killed their wives and children in front of them. And just as our troops arrived, she killed the three guys. She was arrested and placed in my custody."

Standards of morality normally depend on self-regulated behavior, but some psychological mechanisms delink behavior from morality. Bandura refers to "unhooking" or selective moral "abdication."[285] Childhood behavior responds to external rules and social sanctions. Through socialization, each person adopts moral standards as a guide to behavioral self-control. Morality has two components: one component inhibits—giving one the power to refrain from behaving inhumanely; the positive component drives a person to behave humanely. People look to "do the right thing" so as not to subject themselves to self-depreciation.

Moral standards do not remain invariable. Activation or selective deactivation of personal control, influenced by the social environment and psychological factors, allows the same person to behave differently in different situations. Individuals do not normally act unacceptably unless they have somehow been able to justify the action. Moral justification allows reprehensible conduct to become personally and socially acceptable without the need to transform one's personality or values. Redefined morality allows one to undertake reproachable actions free of auto-censure.

In Figure 5 we see the potential junctures where moral self-control can be lost, thereby allowing the justification of inhuman behavior.

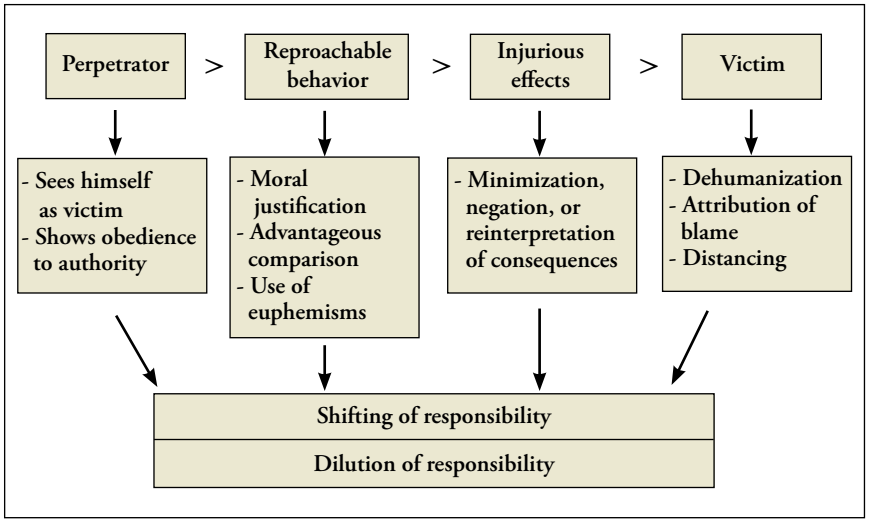


Figure 5 Principal Justifications for Inhuman Behavior

Source: Compiled by the authors, adapted from Albert Bandura, "Moral Disengagement in the Perpetration of Inhumanities," *Personality and Social Psychology Review*, 3, no. 3 (1999), p. 194.

Often, the perpetrator or author of violence considers himself or herself a victim: humiliated, defeated, or treated unjustly. This gives the individual an excuse to attack, whether in self-defense or as a form of reprisal. Obedience to authority and participation in a group effort also spread the responsibility for the action. Reproachable conduct legitimizes itself by appealing to the idea of reciprocity against the actions of the enemy. Because the honor or survival of the group can be at stake, the "morality of results" begins to rule; that is, the end justifies the means. Language helps to soften the meanings of the transgressions, with euphemisms like "defense," "cleaning," "incident," "collateral damage," and "retire." Denying or minimizing actions taken, or discrediting evidence, distorts the meaning of one's actions. One may keep a victim at a physical distance (facilitated by modern weapons) or build psychological distance by assigning the status of being different, a traitor, or unfaithful. If one removes the victim's humanity by resort to a label such as parasite, animal, or the name of a sickness, the action may seem beneficial or even necessary.

In this film the authorities did not anticipate the catastrophic threat and feel embarrassed. As a result, the detainee arbitrarily loses his freedom. One must obey the central authority: "The high command believes that everyone should do what we believe best for our country and its people." The presence of a high-level civilian, a government official, removes responsibility from the military commanders. General Paulson gives orders to Colonel Kerkmejian, and he to his soldiers. But the civilian judge does not have a supervisor, and the FBI agent remains only an observer. The government operation represents a collective effort, carried out by a lone individual (H). The torture appears unacceptable, and perhaps illegal, to some officials. However, they all agree that if the devices detonate, the legal basis for the republic's existence and the rule of law will also have been lost.[286] H sees torture as a tool to obtain information, and the only way to overcome weakness and fear. His euphemistic reformulation of the issue justifies the inhuman treatment because only results matter.

Conclusion

Intelligence management has the obligation to apply public ethics. The "ought," for an intelligence official acting on behalf of a state operating under the rule of law, rests on respect for the dignity of the individual. The professionalism of intelligence services implies the existence of a sound and value-based legal foundation. Capable, internal intelligence management will reduce the growth of "distrusted identities" that encourage poorly considered actions in crisis situations.

The film *Unthinkable* or *El día del juicio final* updates the classic "ticking time-bomb scenario." This scenario sets forth the possibility—or necessity—of extracting information using a variety of brutish methods to save the lives of innocent people. A deep analysis of the film and of the environment of police intelligence finds the film's assumptions highly misleading and far from realistic. Further, a psychological interpretation of the film demonstrates that torture remains unjustifiable as a tool for gathering useful information even in crisis situations.

Some films do offer useful insight into state intelligence practices. They also lend themselves to theoretical and practical interpretation. Both theoretically and practically, intelligence and counterintelligence methods require adjustment to judicial and ethical frameworks to ensure respect for human rights.

Filmography

CONTACTO EN FRANCIA (*The French Connection*), [DVD]. William Friedkin, United States, D'Antoni Productions, Schine–Moore Productions, 1971. (104 min.)

EL DIA DEL JUICIO FINAL (*Unthinkable*), [DVD]. Gregor Jordan, United States, Lleju Productions and Films and Sidney Kimmel Entertainment International, 2009. (97 min.)

EL SECRETO DE SUS OJOS (*The Secret in Their Eyes*), [DVD]. Juan Jose Campanella, Argentina, Tornasol Films, Haddock Film, 100 Bares, Telefe and others, 2009. (129 min.)

QUÉMESE DESPUÉS DE LEERSE (*Burn After Reading*), [DVD]. Joel and Ethan Coen, United States, Bronx Community College, University Avenue at West 181 Street, Bronx, New York City and others, 2008. (96 min.)

LA BATALLA DE ARGEL (*Battle of Algiers*), [DVD]. Gillo Pontecorvo, Italy and Algeria, Igor Fil y Casbah Film, 1966. (121 min.)

LA CIUDAD DE LAS TORMENTAS (*The Green Zone*), [DVD]. Paul Greengrass, United States, Universal Pictures, Studio Canal y Relativity Media, 2010. (115 min.)

LA VIDA DE LOS OTROS (*The Lives of Others*), [DVD]. Florian Henckel von Donnersmarck, Germany, Wiedermann and Berg Filmproduktion, Bayerischer Rundfunk, Arte and Creado Film, 2006. (137 min.)

LOS INFILTRADOS (*The Departed*), [DVD]. Martin Scorsese, United States, Warner Bros. Pictures, Plan B Entertainment, Initial Entertainment, 2006. (151 min.)

An earlier version of this essay appeared in *Las jornadas de derecho publico 2012*, published by the Pontificia Universidad Catolica of Valparaiso, Chile.

Authors' Biographies

Dr. Moira Nakousi Salas practices clinical psychiatry and serves as a member of Chile's Film Rating Council. **Email:** *moira.nakousi@gmail.com*.

Daniel Soto Muñoz teaches and conducts research at the Carabinero Academy of Police Sciences (ACIPOL) of Chile. He also serves as a legal consultant on human rights and humanitarian law. **Email:** *dansotocl@yahoo.es*.

Intelligence, Communications Media, and Political Discourse

Manuel I. Balcazar Villarreal

Effective oversight of intelligence in the democratic context depends on the development of a trusting relationship between those who carry out this governmental function and the political elite, insofar as those elites represent the rights and interests of citizens. To promote the relationship, mass communications media could highlight the strategic importance and legitimate uses of intelligence. This has not happened despite a wealth of opportunities.

In these first years of the 21st century the Western Hemisphere features a complex security environment with internal political crises in various countries. The growth of democratic governance coincides with somewhat greater attention to intelligence services in the region's political discourse. However, even as intelligence has gained attention among the media, and political leaders refer to it more frequently, confusion reigns about the real nature of the phenomenon. Neither the media nor politicians use the term "intelligence" in a way that accords with its meaning in the eyes of specialists in academia or in relevant governmental organizations.

Media often allude to intelligence organizations as security institutions, highlighting their achievements, particularly in "capturing criminals." This tendency may reflect the selective release of information by intelligence directors who seek a positive public image and favorable institutional positioning. This leads to an avoidance of serious public debate about intelligence. Examples may be found in press reports of the capture of presumed drug traffickers in Argentina, Colombia, and Mexico.[287]

Unauthorized disclosure of classified material and insider revelations by active or retired intelligence personnel also link intelligence with communications media. Most often, these incidents occur as a result of someone's resentment toward an organization, their frustration over the internal allocation of resources, or career progression issues. Although leaks do not occur frequently, they have serious repercussions for intelligence organizations, especially because an individual familiar with an organization's operations can fine-tune the disclosure to enhance institutional damage.

Although intelligence leaks might be spread by various communications media, the public often ignores the information. Exceptions occur when leaks concern specific threats such as dangerous criminals, "evil" terrorists, or "disturbed people." Individuals who fit these categories already receive ample attention by the communications media and have gained public notoriety.

The foregoing examples illustrate the media's propensity to deal with intelligence topics mainly in operational terms. Political officials take the same approach, and often use the term "intelligence" in speeches as a synonym for an investigation with results suitable for public consumption. Police forces as well have begun to pass on to the communications media selected details of successful intelligence operations in criminal cases. However, police typically do not share with the media examples of crimes prevented by intelligence actions, or preventive actions taken to reduce crime rates. This perhaps indicates that strategic intelligence thinking remains uncommon among police forces.

The communications media do publish police press releases that emphasize intelligence "actions" taken to reduce criminal activity. These police operations reveal the capture of weapons, ammunition, persons, vehicles, and communications equipment. Meanwhile, we learn little about initiatives taken to monitor or impede financial transactions within or between criminal organizations. Again, if such stories were to appear, the public would see that intelligence capabilities have moved toward the strategic application of technically and operationally complex operations.

Despite the conceptual confusion that surrounds the treatment of police intelligence in the communications media, a clear link exists between the media and the interests of police chiefs. A chief may be able to construct a political career, increase police budgets, or outmaneuver other security agencies by emphasizing the operational view of intelligence. The operational emphasis helps a chief create a public perception of professionalism and lead the public to expect more from intelligence than current capabilities allow.

These circumstances repeat the experience of mid-20th century Central and South American countries. Then, police forces used investigative resources for the political purpose of establishing stability and social control. The circumstances coincided with a limited development of intelligence services, with

an emphasis on its operational rather than strategic side. Physical capabilities took priority over analytic capacity.

A persistent focus on the operational rather than the strategic side of intelligence has generated an empiricism that favors an operational perspective within organizations. In many countries, incoming leaders of the intelligence services perpetuate this tendency because their familiarity with intelligence comes from the aforementioned, selective media reporting.

Media and intelligence interests also converge when political espionage yields a compromising conversation or reveals incriminating video of a political figure. Although government intelligence cannot legitimately target political figures, public scandal ruins careers. The targets of political espionage face the challenge of trying to explain private actions that have now been made public.

Revelations from illegitimate espionage tend to gain traction in the media and therefore spread across a society. As this occurs, a distorted perception of intelligence emerges. A skewed treatment of intelligence by the media overlooks the potential of strategic governmental intelligence. Further, the distorted perception of intelligence generated by the empirical approach of intelligence organizations and reinforced by the media affects how political elites incorporate intelligence in public affairs discourse and the creation of public policy. Political elites consider operational rather than strategic intelligence the society's optimum choice for confronting particular risks or threats.

These circumstances create a challenge for the management of intelligence in the new century. In aggregate, they reinforce bureaucratic inertia in the intelligence services. As a result, those services exhibit a limited capability to improve and professionalize their work.

The principal means of reversing this dysfunctional process among intelligence, the media, and political discourse depends on the media's willingness to establish links with academic researchers who can review specialized literature on intelligence to place government press releases and reports in context. Researchers can also question and evaluate the statements and proposals of political leaders to reduce public confusion about the nature of legitimate governmental intelligence.

Manuel I. Balcazar Villarreal holds a master's degree in public administration from the *Instituto Nacional de Administracion Publica* (INAP-Mexico). He has attended security seminars at the Center for Hemispheric Defense Studies of the National Defense University, Washington, DC, and participated in a crime prevention seminar at the University of Chile. He was an invited participant in the U.S. Department of State's 2008 course on international organized crime. Later, he served as Deputy National Security Director in the office of the President of Mexico. He now serves on the faculty of the *Universidad Iberoamericana*, where he teaches in the national security program. His publications include *La influencia de las maras en México: un problema de inteligencia gubernamental* (INAP, 2007) and *Inteligencia Estratégica en el Contexto Mexicano* (Tecnológico de Monterrey, 2012). **Email:** *ibavil@hotmail.com.*

Section Two
Intelligence Management within the Executive Branch of Government

Presidential Decisionmaking Process and Intelligence—Exploring an Open Question

Guillermo Holzmann

Overview

This review essay identifies the purpose and nature of national intelligence products in Latin America, and stands as part of the author's separate, larger effort to examine institutional biases and defects in the products of a national intelligence system. These products contribute to a decisionmaking process where presidents face basic challenges to political development.

Introduction

Globalization reduces a society's opportunity to grow and develop if it does not learn to adapt economically and politically. Adaptation requires a redefinition and broadening of national interests beyond those classically expressed in official documents.[288] Identifying and analyzing traditional and new challenges over a timeframe that reaches beyond an individual presidential term gains legitimacy with participation by the society's elites. At the same time, this approach requires understanding and acceptance by the society at large.

The developed country perspective on structural change and globalization differs from that of developing countries. For Latin America, the process of globalization demands that leaders confront not only lingering problems from the 20th century (poverty, inequality, ideological confrontation between capitalism and communism, and the permanent search for social development, among other things), but also the challenge of inserting their country fully into the international environment. This challenge calls for opening a country's markets to outside forces. It means that a good government must align itself to an environment that prizes stability and governability.[289] The requirement for adaptation directly impacts decisionmaking processes at the national executive level. A national leader has to respect accrued social and political debts while at the same time establishing a future policy direction through anticipatory, opportunistic decisionmaking.

A state's ability to influence future scenarios by processing and manipulating information has become an essential element of 21st century political

management. These abilities allow the state to affect threats and opportunities into the future. Sophisticated information handling brings national and foreign, state, nonstate, and private interests into the chaotic democratic decisionmaking process.

Latin American countries display notable differences in degree of development and levels of growth. Although they all fit into the general category of developing countries, Brazil has become a regional power. The status of an emerging country depends on its ability to create and consolidate political, economic, and social conditions commensurate with its national interests. One may reasonably suggest that most Latin American countries face challenges similar to those of the regional powers, but they do not share an elevated socioeconomic and political baseline. Countries that share strategic challenges and objectives also need to share in an examination of their strategic intelligence production.

Any country adjusting to globalization needs a national intelligence system. The system needs to create products worth serious consideration as inputs to the national decisionmaking process. To accomplish this objective, a country needs to integrate its different intelligence organizations by specifying what each brings to the table. Intelligence activity in a democratic regime needs limits. Political regulation can ensure adequate controls and procedures for the intelligence system.

Each state in the region has created, modernized, or transformed an intelligence system oriented toward satisfying the needs of its own leader. In the wake of the Cold War, intelligence organizations continued to define internal or external threats as "enemies," thereby highlighting the military character of intelligence. States now face political, economic, and especially conceptual obstacles to establishing a suitable intelligence system. This is particularly true for "emerging" countries. Sound presidential decisionmaking requires systematically constructed intelligence organizations, where military and police capabilities remain necessary but insufficient to address new security scenarios.

The Intelligence-Policy Relationship

The states of Latin America have adopted different evolutionary pathways to their present set of organizations and systems of intelligence. Some derive

from an academic or think-tank tradition, which translates to their following a "Sherman Kent" model. Many have a strong military intelligence influence. In other countries with a long or strong history of dictatorship and human rights violations, intelligence organizations have a political or ideological tone.[290] In general, the public remains wary of the intelligence "culture."[291]

Since the 1980s, each country has developed and modified its intelligence institutions to meet democratic aspirations, as expressed in legislation and in civilian control. In some cases, a country has also created an intelligence organization designed to support the political leadership. Unresolved issues in intelligence management include the question of coordination among 1) those who produce intelligence, 2) the various decisionmakers who would use the intelligence, and 3) proponents of intelligence autonomy vs. executive direction of the intelligence establishment. Imposing efficient institutional and functional linkages (integration) in intelligence allows a country to gain a relative advantage in dealing with harmful events, seizing opportunities, and neutralizing risks and threats at the highest levels of governmental operation.

For intelligence to build an effective and productive relationship with its ultimate users requires that information and analysis be timely, professional, and believable. A national decisionmaker receives information and advice from numerous other advisers and from think tanks, whose purpose is to influence decisionmakers and to advocate certain decisions or simply raise arguments to defend particular interests.

A central point is that the intelligence producer needs to know the stance of the decisionmaker on an issue so as to deliver input suited to the needs of the moment and meaningful for longer-term objectives and priorities. At the same time, because of its nonpartisan nature, and its focus on state objectives as expressed by each political administration, intelligence input should receive special attention over other sources of advice.

A thoughtful decisionmaking process and a suitable institutional framework for intelligence remain a rare combination in the region. A fully functioning intelligence system includes clearly demarcated levels of operation, democratic controls, and adequate resources. When these conditions are met, intelligence operates under the guidance of the highest office holders of the state, and the system escapes the excessive growth of activity by basic intelligence

organizations like those of the military or police. In the absence of a high-level, professional civilian intelligence organization, these basic organizations fill the void by developing not only tactical and operational intelligence, but also strategic and national intelligence, which has the effect of devaluing their principal roles and functions and delegitimizing the idea of a functioning national intelligence system.

For democratic countries with a weak adaptive capability and weak inter-agency coordination, intelligence usage at the highest political level tends to settle into some combination of the following patterns:

1. Personalized and politicized intelligence promotes an official's remaining in power by neutralizing potential political adversaries or justifying short-term political action.

2. Intelligence focuses on the control and neutralization of social conflict or risks, and on ensuring that the current administration remains in power.

3. Political intelligence capabilities exclusively serve the government leaders. Other intelligence organizations fulfill their function with differing degrees of autonomy, performing tasks that do not necessarily coincide with objectives supported by the government in power.

The tendency to assign "politically trustworthy people" rather than the most capable professionals to analytic teams impedes a system's ability to take advantage of long professional experience, to incorporate best practices, and to engage in an ethical approach to intelligence employment on behalf of its users at the policy or political level.

With political trustworthiness a prerequisite for carrying out analysis, intelligence adopts a short-term focus. This focus shortchanges the construction of scenarios and the identification of domestic and international change factors that affect the country's security interests. This situation creates a paradox: Producing intelligence with a short time horizon may help political leaders make reactive decisions in response to current events, but a failure to produce intelligence on issues with a longer time horizon will reduce the likelihood of meaningful contributions to issues of greater importance to the long-term

success of that same political administration. This approach amounts to a deprofessionalization of strategic intelligence capabilities of the state, and a denaturalization of the functions and roles of intelligence organizations at the different levels of the system. The inevitable result: a lack of continuity in the decisionmaking process at the strategic level, and greater costs from constantly changing intelligence management practices.

These circumstances undermine the relationship of intelligence agencies with counterpart organizations in friendly countries. The absence of medium- and long-term analysis impedes a professional exchange of information and analysis on topics of common interest to any two parties. The result is more frequent, informal exchange involving only individual agencies and a growing delegitimatization of the intelligence system because of the correspondingly low standards of professionalization. The implications are many, and although it is not necessarily an express concern of political decisionmakers, a reduction in the international legitimacy of the intelligence system reduces its ability to serve the national interest as an interlocutor on international issues.[292]

Producers of strategic intelligence (at the national or presidential level) do not tend to play a foundational role in the leader's decisionmaking process either in terms of national strategy or national security. In fact, one may even question whether decisionmakers at this level have the ability to use intelligence products. The many questions raised by this observation call for an audit of the process of making strategic decisions.

We need more precise studies of the linkage between intelligence and policy to understand the difficulties inherited from offending political situations of the past, and to identify future challenges. In each country of the region, civilian and military specialists have added to the understanding of intelligence and its implications for policy. Nonetheless, the existing bibliography remains sparse.[293] Important variables to be addressed include the characteristics of the intelligence system, its coordination and guidance, and the ethical and professional standards of its personnel. These variables also relate to challenges in personnel recruitment, methods of analysis, and the ability to generate anticipatory scenarios. Intelligence culture needs to spread to the presidential level through a specialized intelligence bureaucracy in that office. It is important that this bureaucracy be maintained over time so that it can

manage a policy conversation with intelligence organizations, especially with the system's coordinating entity.

A student of intelligence bureaucracy, Ohad Leslau, has reviewed the role of intelligence in the national decisionmaking process at three levels: individual, organizational-bureaucratic, and the state.[294]

At the individual level, he examines how the psychology of specific decisionmakers and intelligence producers influences the prevailing format of an intelligence product. How may an intelligence producer's psychological profile influence information analysis methods and the decisionmaker's perception and use of the product? Some analysts develop intelligence as a professional endeavor and others provide political intelligence. The first type, cautious and methodical, offers a technical and professional opinion, without regard to political considerations. Analysts of the second type give greater weight to factors that define the political scenario facing the decisionmaker. An adviser's ability to relate to the leader's immediate environment promotes a fluid and trustworthy relationship with the leader.

Organizational-bureaucratic studies follow from the theoretical work of Graham Allison.[295] Work reviewed by Leslau finds that intelligence organizations play the same role in government as other state agencies or institutions. An intelligence product exerts influence proportional to the status and prestige of the intelligence agency, as judged by government officials. If an intelligence organization operates close to power and decisionmaking centers like the secretary of state, secretary of the interior, or the office of the president, its influence in the decisionmaking process will be greater than that of other agencies.[296]

Research at the presidential level relates three variables to the influence of intelligence in the decisionmaking process. They are 1) the type of regime, 2) the seriousness of the threat being faced, and 3) the "intelligence culture." Not surprisingly, an intelligence product has greater influence in foreign policy decisionmaking within democratic regimes than in totalitarian or authoritarian regimes. Authoritarian leaders tend by definition to blend or confuse national interests with their own political objectives. The North Korean case offers the clearest contemporary example. In a democratic regime, when the

central values of the state come under threat, intelligence becomes a dominant factor in the decisionmaking process.

Leslau finds that existing studies have difficulty in measuring and explaining the influence of intelligence on national decisionmaking. They fail to develop measurable variables from which one might learn when and how intelligence products actually influence presidential decisionmaking. He argues that such variables can be identified, given the variety of sources and levels of analysis that contribute to intelligence products for national leaders. Leslau also finds that research typically focuses on single, specific cases or a single decisionmaker, leading to unsubstantiated generalizations wrung from the unidimensional findings. A more systematic examination of presidential decisionmaking would take into account that intelligence products designed for executive use feed into the different levels of government. Few products receive presidential attention.

In Latin America, the underdeveloped presidential institution typically includes an underdeveloped office of intelligence. The absent office of intelligence contributes to a lack of relevant input for strategic management of the state and of the government itself. This structural weakness can be addressed by a permanent organization installed at the presidential level to analyze information or intelligence and generate strategically relevant options that go beyond the perceived, short-term needs of the successive governments. Intelligence management in the executive branch of government remains weak in organizational, structural, procedural, and professional terms.

Nevertheless, as a country inserts itself into the international environment, robust interagency coordination and an intelligence system with a set of specialized organizations beyond those of the military and police become mandatory for effective political leadership. Legislators also have the opportunity to mandate strategic intelligence products and a government-wide framework for institutional integration and intelligence management.

Some Thoughts on the Essays in Section Two

The essays in this section will foster debate about intelligence management issues in the region. In suggesting areas for continuous improvement in the

region's intelligence systems, the authors open doors to new mechanisms for executive oversight of national intelligence bureaucracies.

Mariano Bartolome examines the challenges for strategic intelligence in South America. He recognizes the persistence of traditional views of conflict derived from the "realist" school of international relations. The principal axes of interest lie in defensive military capabilities, and more recently, in organized crime. Asymmetric challenges, especially terrorism, narcotrafficking, and trafficking in persons, complicate the strategic assessments that guide national development. Ultimately, his essay explains why any country in the region not only needs to have in place a mature intelligence system, but one that yields products specifically oriented toward national leaders.

Alvaro Venegas explores government economic intelligence, with a focus on Colombia. He recounts the lack of savvy management of the country's economic security in various historical episodes, and argues for a more broadly conceived intelligence system. His proposal envisions the development of an integrated system for economic intellligence, with both horizontal and vertical connections across government and beyond. The system would optimize information processing and would focus on anticipatory intelligence and counterintelligence products. This proposal deserves careful consideration because of its thoroughness and because of the necessary political and social adjustments required for its implementation.

Dan Elkins addresses one aspect of executive branch intelligence management rarely taken into account: He recommends a substantive dialog between intelligence resource managers and congressional representatives on budgetary and programmatic matters. The dialog would include a discussion of prospective resource tradeoffs among intelligence personnel, budgets, and the missions of intelligence organizations. Elkins identifies the tools, language, and practices that contribute to an efficient, transparent discussion of resource allocation. The author's points rest on his considerable personal experience. In Latin America, the implementation of some of his ideas would contribute to the needed professionalism in intelligence activity.

Mario Duarte and Grisel Capo address an issue that will require a good deal of professional reflection about the evolutionary status of intelligence in Central America. Their essay argues for the rejuvenation of civil affairs operations

as part of the changing military intelligence paradigm needed to confront militaristic, criminal threats in the region. They analyze the application of the intelligence function, and particularly the value of military intelligence resources, in states with weak security institutions, prominent social problems, and a structurally inadequate approach to addressing transnational organization crime. Although the particular need in Guatemala may be different from that in other countries, the approach proposed by the authors depicts social intelligence as a facet of economic development. Their new idea employs an intelligence methodology to support strategic planning, where intelligence products are oriented toward consumers who have a variety of crime prevention as well as defense objectives. This essay will generate some controversy because it links internal defense with public security, and accepts the use of intelligence for broad purposes. Despite the authors' titular claim, a question remains whether social intelligence generated by a military organization constitutes a real paradigm change.

Carolina Sancho Hirane examines the possibilities for intelligence cooperation within the Union of South American Nations (UNASUR). She suggests how UNASUR members might emulate some aspects of the European Union's experience in intelligence collaboration. She points out the problems facing intelligence services when they attempt to cooperate, especially in the absence of a tradition of sharing information or analysis within a democratic framework. For intelligence cooperation to succeed requires expertly shaped government agencies, together with a convergent political vision among prospective partners in sharing. These requirements further imply that the traditional threat orientation of intelligence should be combined with an orientation toward identifying opportunities and handling risks.

Merely having intelligence organizations in place does not ensure the creation of useful products for decisionmakers at the highest levels of government. Having an intelligence *system* in place also does not suffice. Every intelligence agency by definition produces or should produce useful information. However, one must always ask who the user of that information might be. Intelligence agencies offer little value without guidelines in place to promote quality analysis and to generate products that suit consumer priorities. Judicial and legislative controls and regular financial audits also play a part in underwriting the efficacy of national intelligence.

Latin American national intelligence exhibits several deficiencies, some of them addressed by the essays in this section. First, strengthening the culture of intelligence among the political elite, and especially among those in government positions, will promote debate and improve proposals to employ intelligence wisely. The best proposals will aim to resolve strategic or structural problems, rather than the short-term issues facing individual governments. Second, a permanent advisory staff would allow for periodically drafting detailed presidential directives to adjust the intelligence bureaucracy.[297] This staff could review the proposals by Bartolome, Venegas and Elkins, for example. This ideally placed, professional staff organization can also produce and tailor intelligence for the presidential decisionmaking process, independent of any other useful information that comes to the president. It is also where appropriate criteria for intelligence efficacy and efficiency can be paired with political, economic, and judicial needs in a normative framework.

Chilean Professor **Guillermo Holzmann** holds a master's degree in political science, and is a doctoral student in American studies, with a specialization in international relations. He teaches at the *Universidad de Valparaíso de Chile and the Universidad Adolfo Ibañez de Chile*. He also serves as director of the *Nodo Chile de Escenarios y Estrategias* (EYE), was a founding member of *Centro Latinoamericano de Globalización y Prospectiva*, and participates in the *Red Latinoamericana de Prospectiva*. He has also served as associate director of the *Instituto de Asuntos Públicos*, and as creator and coordinator of the curriculum for *Metodología de Análisis de Inteligencia at the Universidad de Chile*. He has advised the International Development Bank's Program for the Intelligence Education of Customs Officials. He regularly appears as a commentator on national and international radio and television programs. He also serves as director-member of ANALYTYKA Consultants. **Email:** *guillermo.holzmann@gmail.com; guillermo.holzman@uv.cl*.

Improving Producer-Consumer Relationships at the Executive Level: A Continuing Challenge

Manuel I. Balcazar Villareal

Intelligence services always prefer a good relationship with those who seek out and use their products. Contentiousness in this relationship arises from the different environments in which each "side" operates. The environment and circumstances in which the two sides interact can give rise either to greater mutual understanding or to a conflicted and inefficient process in which both sides blame each other and intelligence cannot fulfill its main role of decisionmaking support.

Organizations and Policies

Although they both perform public service, intelligence producers and consumers represent different social environments. Whereas most producers develop their careers within intelligence organizations, in which secrecy and discretion are hallmark doctrinal principles, politicians mature in a public, open environment with unending dialog and social interaction.

These differing origins highlight a principal difference between their two worlds and affects the relationship between producers and consumers. In contrast with politicians, intelligence services tend to have a well-developed organizational culture that favors the consideration of long-term, strategic issues. Naturally, this cultural preference distances them from an interest in short-term political concerns and the daily crises facing politicians. Politicians nonetheless expect their intelligence services to help resolve daily issues because they attribute extraordinary, even if mythical, capabilities to the intelligence services.

In further contrast with intelligence officials, politicians usually espouse partisan social ideologies, a response to election mandates to resolve particular social needs. In some cases, because of their background or career aspirations, politicians choose to have little or no dialog with national intelligence officials, which can lead the former to develop their own approaches to problems

without regard to intelligence input, thus inhibiting the effectiveness of the intelligence services.

Differences in Time Management

Time management by intelligence officials differs radically from that of politicians. Although intelligence officials, operating within their organizations, have a sense of history and permanence, a political leader can count on only four or six years in which to exert direct influence, and seemingly even less, given the enduring nature of many national problems. This condition confers on intelligence producers and their organizations a sense of transcendence, and perhaps a certain feeling of autonomy with respect to problems, given that they are not required to solve them. After all, such problems can take on political, social, or media overtones that are generally de-linked from the production of intelligence. Political leaders have a greater sense of urgency as they take on crises or national emergencies that need to be resolved quickly.

In this environment, it is normal for consumers to request products that address specific problems. This approach means that producers have to adopt a short or medium-term focus, thereby diverting them from being able to fully develop a strategic intelligence capability in the national context. Additionally, political leaders tend to operate with an eye to resolving problems quickly, in light of their full daily agendas. In this setting, intelligence organizations constitute only a part of a politician's broad information environment, and consultation with intelligence occurs mainly in emergency situations involving security, diplomatic or humanitarian issues.

All this means that national, and even strategic, intelligence capabilities remain devoted to tactical- and operational-level concerns. Intelligence organizations do gain some attention when they prepare responsive products in this environment, but their preferred strategic focus remains comparatively unused. Little space exists for strategic intelligence products because they do not help win elections. A politician typically finds it difficult to capitalize politically on the strategic decisions that might be recommended by intelligence.

Perceptual Dilemmas

The main problem in smoothing the relationship between intelligence producers and consumers lies in the perceptions and expectations each side has of

the other. It seems that there are more missed opportunities for approaching each other than there are realized opportunities.

At times, producers may overly accommodate consumers, given that the budget and health of intelligence organizations depends on the resource decisions made by politicians. For example, intelligence may always agree to a politician's demand for products, without giving due attention to the feasibility, impact, or utility of the product in the eyes of the ultimate decisionmaker. An eagerness to meet a request for a particular product may not support professional development of intelligence capabilities because it makes those dedicated to the production of intelligence appear as "minions" or "accessories" to the power needs of the consumer, rather than professionals dedicated to producing relevant products.

When consumers and intelligence producers communicate and enjoy mutual confidence, a greater opportunity exists for the creation of useful and valued products. On-time delivery and good production qualities play a central role in gaining the interest and attention of a decisionmaker in a particular product.

The perceptions of intelligence held by a particular consumer can help or hinder intelligence bureaucracies. This observation extends to other government offices beyond the executive branch. The legislative branch, in providing checks and balances to executive power, can bring about or update national policy to protect the independence of the intelligence services. However, a legislature may also put in place a restrictive information policy that in the long term may only reduce national intelligence capabilities.

Uncertainties on the part of consumers and producers always lend a contentious air to the producer-consumer relationship. If producers do not receive useful feedback they will not know whether their products were useful in decisionmaking. Consumers rarely know how much detail they could or should know about an issue, a consideration that becomes more critical as the operational level of intelligence becomes more prominent. Naturally, a remedy for some uncertainties lies in improving communication and mutual confidence.

Resolving One Dilemma

Modernizing the concepts and principles that apply to intelligence organizations might bring a broader, cross-cutting (transverse) perspective to the

function. That is, intelligence may usefully expand its scope to interact with state governments and public offices beyond the security and defense sectors. This would create a "second generation" of intelligence to transcend the traditional paradigm of the 20th century, with its centralized focus. It may be that a transversal focus would help strengthen intelligence culture and give it a more solid, socially relevant foundation to reduce the distance between producers and consumers. This broader focus should automatically result in a more strategic approach to producing intelligence. Such products could resonate with the aspirations of politicians who have a mandate to improve lives across a whole country.

Conclusion

Of the components of the intelligence cycle, exploitation and dissemination may have the greatest impact on the relationship between producers and consumer. By temporarily interrupting the cycle at these junctures, the process of constructing intelligence products confers value to this relationship.

Improving the relationship between consumers and producers calls for mutual learning and continuous upgrading of intelligence capabilities. In support of these objectives, both sides have the opportunity to adopt a modern and professional approach to the management of intelligence.

Manuel I. Balcazar Villarreal recently served as Deputy National Security Director in the office of the President of Mexico.

Between Fear and Need: An Essay on Historical Interpretation

Jorge L. Jouroff

The Need for Information

The worldwide globalization process, which does not foresee the end of history but its continuation, gives rise to the same problems we have seen historically, but in another form and at the worldwide level. The information revolution, and in particular the use of the Internet, have made more information publicly accessible than ever before, and at an exponential rate of increase.

The avalanche of information and the need to understand the world call for two countermeasures: ensuring information quality; that is, knowing how to select relevant information; and applying an appropriate analytic methodology or conceptual framework.

New technology brings plenty of information to our attention, but we need to know its meaning, just as any science must know how to understand its data stream. Analysis transforms information into intelligence for elected leaders to make decisions. The inherent complexity of analysis argues that the practice of making decisions need not be based on intuition or supposed "evident truths," but on real knowledge. Strategic intelligence, in its various dimensions, provides real knowledge.[298]

Like all intelligence, the strategic variety also presupposes the accumulation, systematization, and management of knowledge. Strategic intelligence necessarily involves a time period greater than the tenure of one government. It brings some stability to an intelligence system. Stability has a different meaning in different historical periods, but always involves a certain political consensus.

Knowledge Management

If we accept the idea that a government should guide, and not only manage state affairs, objective knowledge of social processes appears indispensable. The production of scientific knowledge presupposes not only the gathering of data, but its interpretation through an ordering process that allows us to

understand the world. Possible tendencies in the development of scenarios become predictable with that understanding, and guide us toward best possible outcomes.

Systematic, long-term, and patient information gathering and analysis distinguish strategic intelligence as a form of *knowledge* production. Knowledge has value for advising not just successive governmental administrations, but more permanent elements of government as well.

The Democratic System of Government

A democratic system needs to maintain a certain equilibrium among the branches of government to guarantee its continuation. The mishandling of power through secret, unilateral, behind-the-scenes decisionmaking characterized the era of empires. Intelligence in the same era did not escape this malaise. Today, greater transparency and civilian control exemplify power sharing among the branches of government and can create public confidence in political and institutional actions. The possibility of failure in the application of checks and balances raises the eternal question: Who controls the controllers?

Self-governance or control mediated by the ethical perspective of government officials provides one possible answer to this question. Ethical actions derive from education and from the responsibility that comes with decisionmaking autonomy within the specialized information and intelligence services. This possibility has been tried with little success in Uruguay.

Another answer to the question would rely on strengthening institutional controls. From executive branch control of its agencies to legislative control of the same agencies, oversight (a term perhaps more suitable than "control") tries to establish a balance between the needs of the government and the guarantee of individual freedom. The concept of oversight implies that intelligence agencies benefit the state and society at large, rather than only acting on behalf of successive political administrations.

The democratic process dictates that whoever supervises government activity needs to understand the full context of that activity. This proviso helps stabilize the precarious balance between necessary secrecy and the protection of democratic rights and freedoms.

An implied equilibrium exists between the democratic system itself and its ability to convince various actors of the societal value of stability. Oversight of intelligence helps maintain stability among the branches of government. However, in order to build effective state agencies, the government's need for information will from time to time prevail over the fear of governmental action.

Latin Americans fear autonomous intelligence agencies, given such agencies' repressive role in 20th-century Southern Cone dictatorships. Importantly, these situations resulted from political decisions, and not from decisions by agencies that "went rogue" or became autonomous, although the risk of that happening always exists. In that era, decisions were made by political actors, first by civilians and then by military officials who were acting as national decisionmakers.

The democratic vision can prevail when intelligence activity is held in check, even as the rights of the intelligence system itself are respected. Government does require a strategic perspective from new or redesigned intelligence agencies.

Brief Comments on the Substantive Essays

This book contributes directly to the debate about intelligence in a democracy, without succumbing to the taboos of earlier years. It completes the contribution of two earlier works on the professionalization and democratization of intelligence in the Americas.[299]

The essays in this second section of the book demonstrate the variety of ways in which the management of intelligence agencies has developed, with attendant problems and solutions. At the same time, it manages to address issues in a way that goes beyond the individual concerns or nationality of the numerous authors.

Strategic Intelligence

The Argentine Mariano Bartolome begins his essay with a stirring observation: With only minor exceptions, no real strategic intelligence production exists in all of the Southern Cone. He points out that in the era of dictatorships, intelligence likewise existed only for operational purposes. This does

not mean that intelligence personnel could not produce strategic intelligence, only that the government did not invite their input to decisionmaking.

The problem of poorly developed strategic intelligence relates to its definition. Bartolome acknowledges three competing definitions from the Argentine experience. Intelligence becomes strategic in three different situations: 1) when the product depends on inputs from other, separate organizations or agencies (military organizations, for example, in the case of civilian-produced strategic intelligence); 2) when the product addresses issues of medium- or long-term concern; and 3) when the product takes on particular importance or relevance. To simplify the concept, strategic intelligence informs a country's highest-level decisionmakers and transcends immediate circumstances to identify long-term threats and opportunities, whether existing or potential.

Brazil offers a good example. This country's national development traces to the so-called "Sorbonne School" of authors who thought of their country in geopolitical terms. This perspective was projected particularly by Travassos and by the military men Golbery Da Couto e Silva and Meira Mattos.[300] Similar initiatives appeared in Argentina and Chile.[301] In Chile, naval officials engaged in geopolitical thinking, but in contrast with Brazil, this country did not have the material basis for transformng such thinking into physical and political reality. Southern Cone geopolitical thinking took place in consonance with global power shifts. With its continental proportions and persistent geopolitical outlook, Brazil became identified with this school of thought. It also combined short-term with long-term planning, starting with the 1964 military coup and continuing to the present. Bartolome notes that Brazil has continued its geopolitical thinking and has put in place a set of strategic-level governmental agencies.

Although only the larger and more powerful countries have developed a framework for strategic intelligence, globalization makes it a useful tool for all countries. Paraguay and Uruguay have begun to reshape their defense and intelligence sectors with an eye toward establishing strategic thinking. As noted in Bartolome's essay:

> Strategic intelligence provides a fundamental tool for the modern state to prevent, combat, and neutralize transnational threats. These threats "require enhanced understanding,

> information and analysis, presented in a timely and efficient manner to policy framers who can then make the best decisions." Luis Alberto Sallaberry, head of the Brazilian intelligence agency (ABIN), summed up the role of intelligence as "strategic counsel" to the president of the republic.

The advisory role underlines the idea that strategic intelligence fulfills an *analytic* rather than *operational* purpose.

Latin America does not enjoy an abundance of highly trained human resources, but it does have the capability to develop human intelligence and to structure interagency cooperation inside of each country and regionally to optimize intelligence capabilities. The organizational framework for intelligence production affects those capabilities. Bartolome captures these effects succinctly: "Whatever shape cooperation may take will be influenced by the structure of the intelligence organizations involved. Do the agencies in a community engage in collaborative tasks, or alternatively, do they form a system where a lead agency exercises control over cooperation or collaboration?"

Typically, several intelligence agencies operate within a single country, but not as a coordinated system or community. A community suggests something beyond the mere existence of a set of agencies, to include coordination and complementarity, as well as interconnections among the constituent parts. A community also suggests the existence of an information collection plan at the national level, with attention to defined priorities.

Another question to resolve is whether an intelligence system can maintain continuous coordination, or whether the coordination will require an arrangement whereby one particular agency will become the "lead" organization. The various alternatives and their implications are now under discussion in legislative chambers across the region.[302] The debate about intelligence organization design or redesign can also involve the areas of defense and security, with repercussions for a variety of government organizations, to include the possibility of their resubordination.

The essay by the Colombian Alvaro Venegas addresses government economic intelligence, or "the knowledge resulting from collection, compilation, evaluation, dissemination and protection of information related to national and

international economic phenomena and actors." He expressly differentiates economic intelligence from economic espionage. Economic intelligence requires the formation of governmental analytic teams as a way to contribute to decisionmaking at the national level.

He expands the classic intelligence cycle of collection, analysis and dissemination by adopting a theory of intelligence developed by Jennifer Sims. Sims adds the functions of anticipation and manipulation to the cycle to incorporate the concept of outwitting and weakening the adversary. Venegas concludes that "Sims offers a systematic means of measuring success in intelligence activity, and for evaluating an intelligence case study."

The Venegas essay aims to make the value of economic intelligence apparent to government decisionmakers. His essay demonstrates to any reader that intelligence should not limit itself to the classic or traditional concept of "security threat," but instead encompass a country's economic health. Intelligence can help identify opportunities and sketch possible scenarios to ensure economic health.

Dan Elkins, an experienced practitioner, presents a careful and pragmatic outline of steps toward achieving accountable financial management of intelligence resources. His approach presumes the existence of a sophisticated resource management system, like that of the United States. Latin America has no equal in terms of resources devoted to the intelligence mission. Thus, his concepts conform only to the North American reality. Still, he is able to solidify for everyone the idea that financial resources management treats an intelligence budget as a "numerical expression of policy preferences." Elkins's "business" approach to financial management decisionmaking for now remains at odds with typical practices in the southerly latitudes.

If South American bureaucrats prove themselves able to apply his method adaptively, and not merely copy it, they will have implemented his artful guidance. Elkins's four levels of financial management guidance correspond precisely with the governmental management levels Goncalves identified in the first section of the present work: 1) agency—internal to a particular intelligence agency; 2) executive—carried out within the executive branch by nonintelligence entities of the administration and by the department or ministry to which the intelligence agency is subordinated; 3) external—exerted

by the judicial branch, by the legislative branch, and/or by an independent entity; and 4) popular—where the concerns of individual citizens or civil society organizations are addressed.

Elkins also distinguishes between effectiveness and efficiency. South Americans are accustomed to measuring success by the outcome of a mission, regardless of the costs that go into achieving it. Elkins poses a series of questions whose answers indicate both *effectiveness* of operational success and *efficiency* of budgetary management. Efficiency applies to the use of appropriated and obligated funds. Together, effectiveness and efficiency bring continuity to the management of intelligence. As Latin American countries continue to build or redesign their intelligence systems, incorporating experiences from outside the region should prove useful.

Grisel Capo and M. Duarte write about the historic antisubversive role of a Guatemalan military civic-information program in the mid-20th century. It contributed to the government's strategy to win popular support. The program ended with the establishment of a military dictatorship. The authors show how the civic-action program began as a specialized intelligence effort to study the social conditions of the population. Although it operated under the banner of the infamous "national security doctrine," the program aimed to prevent violence.

The authors propose that the Guatemalan government reinvent this early experience by applying social intelligence against new threats such as narcotrafficking. They suggest that police responsibility for prevention of violence in local communities be reallocated to the armed forces, given the elevated level of social tension that now exists.

Carolina Sancho Hirane of Chile traces nascent intelligence cooperation within the Union of South American Nations (UNASUR). The emergence of intelligence cooperation has to contend with the variety of national establishments, each with different missions. Nonetheless, two realities spur cooperation: growing globalization obliges each country to share information, and most countries share the same threats and challenges.

Cooperation depends on regional agreements and alliances to make it viable. Regional and bilateral cooperative agreements at times overlap with

arrangements sponsored by international organizations. Two subregional alliances operate in this way: the Common Market of the South (MERCOSUR) and the Andean Community of Nations (CAN).

Sancho Hirane compares the status of intelligence cooperation in the European Union (EU) with that of MERCOSUR. MERCOSUR features nascent cooperation in criminal intelligence, which she distinguishes from antiterrorism cooperation. She points to the American Police Community (AMERIPOL) and the Latin American and Caribbean Community of Police Intelligence (CLACIP) as candidates to spearhead the deepening of intelligence cooperation, although she notes that the influence of these two multilateral organizations on governmental intelligence cooperation lacks strength because their cooperation does not take place as part of a political process. EU intelligence cooperation, in contrast, has grown because of a convergent political environment. Post-World War II customs unions and mutually beneficial industrial development combined with a U.S.-sponsored European alliance (NATO) to create a framework for cooperation. The alliance involved mutual defense policies and therefore, intelligence cooperation. All of this occurred despite the changing missions of intelligence through time, precisely because the idea of a united Europe remained in place.

Because unique national interests do not disappear in the midst of common interests that stem from globalization, cooperation can and should be widespread but never absolute (or unlimited, as Sancho Hirane says). Cooperation in intelligence includes not only the exchange of information but also the capability to work together for the sake of common interests. In Latin America, the process of intelligence cooperation that began with bilateral agreements, and that has evolved through MERCOSUR and more recently, UNASUR, remains stable and under construction.

Jorge L. Jouroff studied economics in the Department of Economic Sciences and History at Uruguay's *Universidad de la Republica*. He has served as a representative on the Central Program Committee of the *Frente Amplio* political party, and as member and adviser to the committees on national defense and citizen security of the Uruguayan Congress. He has been director general of the Secretariat of the Ministry of the Interior and has worked in the office of the President of the Republic for the National Emergency System. He has also worked as general manager of SEMEJI (special justice program for

juveniles) and served as an adviser to the United Nations Development Program. Presently, he is a professor at the Police School for Advanced Studies (*Escuela Policial de Estudios Superiores*). He is also a private-sector consultant. His work includes the book *Public Security and Human Rights* [*Seguridad Pública y Derechos Humanos*] (Montevideo: *Ediciones de la Banda Oriental*, 2005) and an essay on "Intelligence and Culture: A Proposal for Uruguay," in *Democratización de la función de inteligencia* (Washington, DC: National Defense Intelligence College, 2009). **Email:** *admijor@adinet.com.uy* and *jorgejou@yahoo.com.*

Strategic Intelligence Requirements for the Security of Latin America

Mariano Bartolome

Introduction

In South America, national intelligence receives little attention from social scientists. In the author's home country of Argentina, with the exception of Ugarte's work, the few academic works address police or tactical intelligence and business intelligence.[303] Because of this inattention, citizens remain ignorant of what intelligence is, and have only a distorted collective image of what it can be.

A predominantly negative perception of national intelligence certainly comes from state intelligence organizations across the region having operated in the 1980s as instruments of the country's authoritarian regimes. These organizations led the way in violating the civil rights of individual citizens.

The democratization that began across South America about three decades ago has facilitated civilian control over intelligence organizations, to include the training and education of specialists and the design of a professional career path for those who remain employed as state functionaries. Nonetheless, the region lacks a political culture to sustain the legitimate role of intelligence in democracy.[304]

Despite the consolidation of democracy across much of South America, a distorted view of intelligence remains in place. This view sees agencies using publicly funded human, financial, and material resources to achieve goals associated with short-term objectives of the regime in power rather than in support of national interests. Further, in the popular imagination, intelligence organizations remain exempt from the application of controls and the corresponding accountability characteristic of a healthy democracy.[305]

Intelligence-related news feeds these perceptions, as when the Brazilian Intelligence Agency (ABIN) began, without judicial authorization, to intercept telephone conversations of the president of the republic and members of the Supreme Court.[306] In Venezuela the Bolivarian Intelligence Service (SEBIN) made the news for intimidating and harassing European legislative officials

who had come to this Caribbean nation to monitor the transparency of national elections and the freedom of expression of communications media not aligned with the government.[307] SEBIN, under the guidance of Cuban intelligence specialists, also allegedly intercepted emails of thousands of Venezuelans and their countrymen living in Miami. Intelligence collection targets included activists, newspaper reporters, military officials, Venezuelan diplomatic officials working abroad, and known opposition leaders.[308] The most notable case occurred in Colombia, where the Administrative Department of Security (DAS) took part in internal espionage against dozens of congressional officials and officials of the opposition *Polo Democrático and Partido Liberal*, as well as judges and civil society leaders. Of three DAS ex-directors prosecuted for internal espionage, one received 25 years in prison.[309]

A careful definition of intelligence would establish the reach and limits of the concept and combat negative perceptions of intelligence based on poorly informed judgments. A recent definition declares that intelligence "supplies processed information in a timely and useful fashion about a specific situation, and optimizes the decisionmaking process." In other words, intelligence activity provides a consumer not only information, but also some specific *insight* that allows a reduction in uncertainty, thereby facilitating the decision process.[310] Specific acts of compilation and analysis build an informational pyramid from a base of raw data to an apex of well-considered knowledge.[311]

When this process refers to the actions of a government, one can employ the labels "national intelligence" or "state intelligence," terms widely understood and agreed to across South America. However, any consensus disappears with the introduction of the term "strategic intelligence."

State intelligence activities exhibit extreme differences across South America. The differences arise from the nature of organizations involved (including police agencies); the degree of control over intelligence by the legislative branch; the relationship of the judicial branch to intelligence (in restricting intrusive intelligence actions); and degree of military participation in internal intelligence activities.[312]

What makes intelligence "strategic"? From the author's Argentine experience,[313] the adjective applies in three different situations. First, when the intelligence product depends on inputs from other, separate organizations or

agencies, as when the organization charged with strategic intelligence production lacks the capability to gather the needed information, instead depending on intelligence created previously by institutions that make up the intelligence system or community. Second, when the product addresses issues of medium- or long-term concern; and third, when the product takes on particular importance or relevance. Strategic intelligence informs a country's highest-level decisionmakers and transcends immediate circumstances to identify long-term threats and opportunities, whether existing or potential.[314]

Given their diverse environments, not all South American countries produce strategic intelligence. Even among countries that do, the product may not be so labeled, and the institutions responsible for it display notable differences from one another.

The particular characteristics of strategic intelligence activity in South America influence the approach taken in the present essay, which addresses the following question: What explicit and implicit requirements exist for strategic intelligence efficacy in any South American country?

The Dynamic Security Environment of South America

South America takes two approaches to security, depending on the analytical lens employed. From the traditional, Westphalian point of view, security questions center around inter-state dialog, and the military plays a key role. This model avoids the truly multidimensional nature of the security phenomenon. The security environment appears much less peaceful when viewed in nontraditional or unconventional terms.

Three traits characterize unconventional threats: nonstate actors take the lead; they do not always use violence to carry out policies; and when they do employ violence, it occurs outside of the traditional formats of Clausewitzian logic. That is, conflict becomes asymmetric or heterogenous. Heterogeneity develops through a process of "securitization,"[315] defined as "strategic uncertainty" or the "globalization of fear."[316]

When dangers or threats have no clear origin and no territorial or political limits, the perception of insecurity becomes permanent, touching all individuals in a society. As a function of their scale of operations as well as their complexity, terrorism and organized crime dominate the South American scene,

and their identities and actions blend together. As an example, the Peruvian *Sendero Luminoso* (SL) turned from terrorism to narcotrafficking in the mid-1990s, but then reverted to their original practice of armed action in the Valleys of the Apurimac and Ene Rivers (VRAE). They also confirmed their transnational nature by extending operations outside of Peru as they began to engage in bank robberies in Bolivia and sell drugs in low-income suburbs of Buenos Aires.[317] The Revolutionary Armed Forces of Colombia (FARC) also conduct complex transnational criminal operations. Evidence for this claim comes from information found on personal computers retrieved by Colombian forces in the March 2008 raid on a FARC camp in Ecuador.[318]

Other groups in the region whose goals and operational capabilities remain unclear also resort to violence. Among them are the Revolutionary Cells of the Mauricio Morales Brigade in Chile; the Carapaica Revolutionary Liberation Movement of Venezuela; and especially, the Paraguayan Popular Army (EPP). The EPP includes prior members of the *Patria Libre* party, and though they adhere to Marxist-Leninist principles, their actions center on obtaining money by kidnapping prominent cattlemen.[319]

According to the Organization of American States, criminal violence has attained the status of a "pandemic" that annually costs the region's citizens more than $16 billion in U.S. dollars. Although the region holds only 8 percent of the world's population, it accounts for more than 40 percent of homicides and almost 70 percent of the planet's annual total of kidnappings for money.[320] A nongovernment organization that specializes in urban violence finds that 24 of the 25 most violent cities in the world are in Latin America. The list is headed by the Honduran city of San Pedro Sula, with a homicide rate greater than 159 cases per 100,000 inhabitants.[321]

Each criminal organization in Latin America exhibits a different level of intensity. The illicit production and trafficking of drugs stand out as especially intensive activities. The region produces the entire world's supply of cocaine in addition to marginal amounts of heroin and cannabis. The United Nations Office on Drugs and Crime (UNODC) claims that the land area devoted to the illegal cultivation of coca amounts to about 149,000 hectares (368,000 acres—about the area of a typical county in the United States—although of course the dispersed distribution of the coca-producing fields makes that comparison misleading. Of this total, 41 percent is in Colombia, a percentage

similar to that in Peru, with Bolivia accounting for the remaining 20 percent. Of course, the cocaine produced by these three Andean countries represents only a small share of worldwide illicit drug production. Although the value of the region's illicit commerce can only be estimated, the UNODC calculates the street value of South American cocaine as between $75 and 100 billion annually.[322]

This transnational narcotrafficking scourge and the violence that accompanies it continues to expand. Beyond FARC and Sendero Luminoso involvement, "emerging criminal groups" of Colombia (known as BACRIM) and criminal cartels of Brazil have entered the picture. The government of Colombia categorizes BACRIM as a new, armed enemy of the state. Narcotrafficking remains the foundation of their criminal activity, today involving about 7,000 recruits, about the same as the FARC.[323] The crime cartels of Brazil, meanwhile, operate in the favelas of important cities. From those strongholds, they manage drug trafficking, with active interest in prostitution, gaming, arms trafficking, contraband, and extortion. Sao Paulo's *Primer Comando de la Capital* (PCC) and Rio de Janeiro's *Comando Vermelho* (CV) have become especially notorious.

Arms trafficking in Latin America also creates a clear transnational impact. The Center for Defense Information of Washington, DC estimates that up to 80 million weapons—half of the world's illegally transferred arms—are in circulation in Latin America.[324] Illegal arms flow to South America from diverse source countries. Some come from parts of the former Soviet Union (especially Eastern Europe); some come from other parts of Europe. To a degree, these pathways reverse cocaine-trafficking routes to the Old World. Entry points are usually the port cities of Brazil, Venezuela, Ecuador, Panama, and especially Nicaragua. Arms transferred illegally from military and police arsenals across the region add to the totals. They are stolen from government stockpiles or purchased directly from government officials.

Illicit transfers add variety to the inventory of arms in the hands of terrorist and criminal groups operating in South America. The arms range from handguns and submachine guns to modern rocket launchers such as the *Saab Bofors* AT-4 (which have been captured from the FARC). Various 5.56 mm and 7.62 mm assault rifles join MAG-30 Russian antiaircraft machineguns and RPG rocket launchers. Sendero Luminoso uses rocket launchers to down

military helicopters. The capture of worldwide arms merchants Monzer al-Kassar and Viktor Bout, in 2007 and 2008 respectively, allowed us to understand the levels that this illegal trade could attain in South America when international mechanisms for detection and interdiction fail: *Strela-II* and *Igla* portable antiaircraft missile launchers (MANPADs) of Russian origin now complement the FARC arsenal.[325]

Although South America plays only a marginal role in human trafficking, it remains an especially vile scourge. Human trafficking sends people from South America to North America (the United States and Canada), Europe (especially Spain, Italy, and France), as well as to Asia (Japan and Korea).[326]

Strategic Intelligence and the Security Challenge in South America

Public policy will benefit from optimized strategic intelligence. Strategic intelligence can prevent,[327] combat, and neutralize transnational threats. These threats "require enhanced understanding, information and analysis, presented in a timely and efficient manner to policy framers who can then make the best decisions."[328] Luis Alberto Sallaberry, head of the Brazilian intelligence agency (ABIN), summed up the role of intelligence as "strategic counsel" to the president of the republic.[329] In general, the countries of South America have begun to acquire an adequate strategic intelligence capability.

Paraguay offers an example of this trend. President Lugo ordered defense modernization and a review of its responsibilities, including creating an organization suitable for carrying out strategic intelligence. Responding to this presidential directive, for the first time the Defense Ministry established an intelligence curriculum for the armed forces. The coursework aimed to prepare military personnel to combat organized crime activity by the Paraguayan Popular Army and others. In inaugurating the intelligence course, General Lezcano Davalos, director of the Senior Strategic Studies Institute (IAEE), explained that "[t]he purpose of this course of study is to professionally prepare the specialized human resources needed to confront emerging threats."[330]

In Uruguay, the National Defense Law of 2010 has reinforced the push for modernization. This law provides a framework for actions by the General Staff of the Defense Ministry (ESMADE), as well as for the police-oriented

National Information and Intelligence Directorate (DNII) of the Interior Ministry. The leader of ESMADE now has the duty to use intelligence capabilities to alert political authorities about threats to the well-being of the state. Those intelligence capabilities reside in the National Directorate for State Intelligence (DINACIE), created in 1999 within the Defense Ministry. Among other things, ESMADE is to monitor narcoterrorism, large-scale migration, health epidemics, threats to the natural environment, trafficking in humans and human organs, the breakout of conflict generated by social inequality, the increase of marginalized populations, arms trafficking, large-scale electronic funds transfers, the transport of toxic waste, technological terrorism, and industrial espionage.[331]

The DNII's chief officer has acknowledged that the production of strategic intelligence now constitutes its main mission. In the eyes of the DNII, strategic intelligence identifies risks and threats to the liberties and rights of citizens, the well-being of the state, and the stability of democratic institutions. This type of intelligence contributes to a government strategy that minimizes or avoids risks to the interests and sovereignty of Uruguay.[332] Curiosly, the head of the DNII believes that his institution owns the requirement, even as DINACIE, by most readings, has the obligation to produce strategic intelligence for the country.[333]

The internal espionage scandals that surrounded Colombia's Administrative Department of Security (DAS) resulted in its dissolution by President Juan Manuel Santos. The new agency replacing the DAS is the National Intelligence Directorate (DNI). As a civilian institution under the authority of the president of the republic, the DNI, in contrast to the old DAS, carries out intelligence and counterintelligence functions only. This specialization should allow for the development of a strategic intelligence perspective. The DAS's other functions have been transferred to other state institutions. The Technical Investigatory Corps (CTI) of the attorney general's office, the Ministry of the Interior, the Ministry of International Relations, and the National Police now employ thousands of reassigned DAS employees.[334] Many of the former DAS employees provided VIP protection and immigration control.

It remains difficult to envision a single, typical strategic intelligence model for South American countries because of the heterogeneous intelligence institutions across the region. However, the present review finds some common

ground in four basic conditions that need to be met by strategic intelligence institutions in South America, if those organizations expect to address the transnational threats that cloud the security horizon.

1. Recapitalization of human intelligence (HUMINT) will certify its importance even as technological advances boost the value of signal and image sources—both mainly satellite-based. Limitations and prerequisites do exist for capturing signals or obtaining images through technical means and can be overcome by human sources. Images and signals collected by technological means have intrinsic value, but remain insufficient for assessing the political meaning of information. HUMINT information often provides the data necessary for imparting a critical understanding of the principal independent variable in any analysis at the strategic scale. HUMINT is generally the best way—and sometimes the only way—to obtain information about actors who make decisions within a restricted circle. Small groups can develop plans in a secretive and self-serving way, penetrable only by long-term intelligence operations.[335]

Colombian experience in combating the FARC illustrates the importance of an adequate HUMINT capability, complemented by signal and image intelligence. Some examples include the takedown of Raul Reyes (Operation Phoenix-March 2008); Jorge Briceño (Operation Sodoma-September 2010); Alfonso Cano (Operation Odysseus-October 2011); and the rescue of ex-presidential candidate Ingrid Betancourt (Operation *Jaque*-June 2008).

The controversial Operation Phoenix grew from a complex intelligence operation. Intelligence preparation began in February 2007, when the Colombian National Police activated seven special groups. The groups acted separately to locate each member of the FARC Secretariat. One of these teams moved to Putumayo, near Ecuador, because of Reyes sightings there. Patient intelligence work began to yield results when an undercover agent gained the confidence of a security team protecting the insurgent chief.

Accumulated knowledge of Reyes's location and activity indicated the imminent creation of an insurgent camp on the Ecuadorian side of the border. Colombian agents obtained and monitored the satellite telephone number used by the guerrilla group, and fixed the camp's location. The Colombian Air Force launched laser-guided bombs, followed by helicopter-borne army and police commandos.[336]

2. To counter transnational threats, strategic intelligence requires two types of institutional cooperation: 1) between institutions or agencies within a state, and 2), between two or more countries, either directly or within the framework of an international organization. In the first environment, intelligence analysis requires shared interdisciplinary interpretations to capture the complexity of an issue.[337] This helps limit analytic distortions that can arise from allegiance to traditional viewpoints or groupthink.[338]

Intelligence cooperation reflects the structure of the organizations involved. Do the agencies in a community engage collegially, or does a lead agency exercise control over cooperation and collaboration?[339] The degree of centralization in an intelligence system also represents an important variable.

South American initiatives contribute to the deepening and optimization of interagency cooperation in intelligence. Three concrete examples come from Colombia, Ecuador, and Uruguay.

Uruguayan President Tabare Vazquez's administration created the post of national intelligence coordinator in the office of the president of the republic. The coordinator has access to all information available to the state's intelligence organizations.[340] An ad hoc commission in Ecuador found that the Intelligence Directorate of the Armed Forces Joint Command had demonstrated weak intelligence capabilities in 2008 because of the lack of coordination among military elements. The report generated structural reform in Ecuador, highlighted by the creation of the National Intelligence Secretariat (SENAIN).[341] Colombia then created a National Security Council, reporting directly to the president of the republic. It coordinates the intelligence work of the Ministries of Defense, Foreign Relations, Interior, and Justice.[342]

Security in any country is now a shared responsibility among friendly states. The United Nations also promotes cooperative action in international security.[343] A cooperative approach to global security rests on three pillars: that today's threats do not recognize or respect national borders; that the sources of threat are interconnected; and that they need to be confronted simultaneously on the national, regional, and global levels. No one state can make itself invulnerable to unconventional threats by trying to protect its own population and remaining unconcerned about the consequences for its neighbors.[344]

Peru leads the region in adopting the concept of shared security. When Mexican criminal cartels became more active in Peru, the executive branch fostered intelligence cooperation between Peruvian agencies and their Mexican counterparts.[345] The Peruvian government also pressed for international intelligence cooperation at a Lima meeting of the Chiefs of Organizations Responsible for Combating Illegal Drug Trafficking in Latin America and the Caribbean (HONLEA). At the meeting, the Peruvian President urged the creation of cooperative mechanisms for the region's intelligence systems to stop the international transfer of narcotrafficking.[346]

The Triple Frontier region also offers a concrete example of multilateral cooperation in strategic intelligence. Following the Argentine terrorist attacks of 1992 and 1994, Argentina, Brazil, and Paraguay established a Tripartite Command to improve security in the Tri-Border Region through police and security cooperation among the three countries. Later, Uruguay and Chile also participated as invited members in ongoing cooperative efforts against narcotrafficking, contraband, document falsification, illegal funds transfers, trafficking in humans, and terrorism.

An "intelligence roundtable" spearheaded regional cooperation. By 2006 it had evolved into a more formal Regional Intelligence Center. Team leaders of intelligence units from these countries worked together in the center to share sensitive information and coordinate covert operations. By thwarting illicit business activity, the Tripartite Command intended to force terrorist and criminal organizations to disband their cells and networks in the region, and to move on to other locations.[347]

Together with the Tripartite Command, 15 Joint Coordination Units (UCCs) operated at specific points along the borders between Argentina, Paraguay, Brazil, and ultimately Uruguay. These units continue their work, staffed by police or other security forces deployed along both sides of the border. The chiefs of each unit carry out the daily information coordination. Like the units associated with the Tripartite Command, the UCCs exchange information to prevent and control local transborder criminal activity as well as organized crime.[348]

Five years after the first multinational security initiative in the Tri-Border Region, Argentina, Brazil, and Paraguay formed the "3+1 Group," with the

United States as the fourth member. This development added a global perspective to a cooperative endeavor that until this time had a glocal profile.[349] Its purpose was to exchange information about terrorism and organized crime in the region, to share points of view, and to develop mutual confidence with respect to intelligence targets. The multilateral effort has also focused on developing a preventive strategy toward crime.[350] The Regional Intelligence Center mentioned earlier increased the level of cooperation among the four countries, especially through targeting international terrorists' logistics and financing.

The 3+1 arrangement shows the importance of multilateral intelligence cooperation with extraregional actors. Another innovation came to light at the fifth summit of the Latin American and Caribbean Police Intelligence Community in 2010.[351] There, the Mexican government offered to share its *Plataforma México* with this community's members. This large database contains the "Combined Criminal Information System" for all of Mexico. The offer promoted the concept of a continent-wide fight against organized crime, spurred by the expansion of Mexican-based criminality to other parts of the region.[352]

3. High-quality intelligence products for decisionmaking must account for complex scenarios.[353] The value of any strategic intelligence product comes from its offering more than the analysis of an issue and the projection of its probable evolution. It needs to contribute to the design of realistic, alternative pathways toward the decisionmaker's objectives.[354] Meeting this expectation depends on the status of two earlier conditions: high-quality HUMINT and fluid interagency and intergovernmental cooperation.

The ability of strategic intelligence to understand, prevent, and manage new threats also rests on a renewed application of academic disciplines and fields of knowledge that in other eras have had only marginal importance. Anthropology, history, the comparative study of religions, and sociology, among other disciplines, have regained utility for strategic assessment.[355] Many aspects of the issues high on the contemporary international security agenda remain nontransferable from one region or country to another. The factors that contribute to interstate conflicts or transnational threats force us to avoid generalizations and inappropriate application of culturally based standards. The strength of cultural factors also limits the applicability of historical analogies.[356]

Open Source intelligence (OSINT) continues to improve its worth for strategic analysis and assessment. A focus on open-source exploitation brings greater appreciation for specialized information from various sources and in different formats. As part of the mixture of OSINT sources, "outsiders" or individuals with deep knowledge of specific topics provide new and valuable points of view to the intelligence matrix. Their inclusion also contributes to a more certain reduction of the cognitive distortions that often accompany analysis.

An example of a high-quality analytic product based on HUMINT, interagency cooperation, OSINT, and outsiders comes from Colombia, where the Ministry of Defense produced its "Defense and Security Statistical Summary 2003–2009" as a public reference document. The document records the government's fight against criminality and terrorism over this seven-year period. It also presents data and identifies trends for selected crimes (kidnapping, for example), terrorism, narcotrafficking, and other forms of organized crime.

According to the Colombian Ministry of Defense, publishing this document improved data handling and storage, the design and application of analytical methods, tracking and evaluating the actions of officials, and notably, the process of decisionmaking within the ministry and at the political level. Furthermore, it promoted the interaction of government with the academic world, so that academia could participate more readily in the design of public policy for security and defense.[357]

4. Production of strategic intelligence rests on an ability to imagine future scenarios focused on medium- and long-term trends rather than only reporting on current, pressing issues. Nongovernment organizations have for decades produced such predictive assessments. They vary from confidential reports on momentous issues to strategic appraisals available to the public. A recent contribution to this genre bears the title "The Next 100 Years." In it, the futurist George Friedman envisions scenarios for the second half of the current century.[358]

Far from being a resource reserved for academics or business people, strategic intelligence practitioners use medium- and long-term assessments to reduce the margins of uncertainty that confront decisionmakers. The National Intelligence Council (NIC) of the United States, a government organization

coordinated by the Director of National Intelligence, analyzes and assesses international issues for the highest levels of the executive branch. In 2008, the NIC published an openly available study of the principal issues driving the international agenda.[359]

Strategic intelligence can produce forward-looking analyses of nontraditional threats that weigh on Latin American societies. It can sound an alarm and contribute to the creation of contingency plans for appropriate actions.[360] In that context, medium- and long-term intelligence estimates promote steady and coherent national security and defense policies and strategies. When those policies continue beyond one political regime, governments can contend with the scourges of terrorism and narcotrafficking.[361]

Conclusion

South American security issues remain susceptible to two different interpretations. Realist theory focuses on established relationships among Westphalian states, and emphasizes the military dimension of national power. Low levels of conflict define the region's political geography. Strong institutions such as the South American Defense Council (CDS) reinforce this interpretation.[362]

The other interpretation finds that asymmetric threats imposed by nonstate actors better characterizes the South American security environment. Two asymmetric, transnational threats stand out for their scale and seriousness: organized crime and terrorism. Geographically, they take advantage of the gray areas wherever fragile governance exists.

Great differences in the intelligence institutions and systems of the region make it difficult to propose a specific "best model" of strategic intelligence to address asymmetric threats. Nonetheless, strategic intelligence production anywhere in the region rests on four pillars: first, adequate attention to and use of human sources, even as more technological intelligence-collection options become available; second, a high level of interagency and intergovernmental cooperation, especially when common interests exist on particular issues or in geographical areas; third, generation of a high-quality product, suitable for use in high-level decisionmaking; and finally, the ability to create medium- and long-term predictive scenarios to guide high-level political decisionmaking.

Putting these pillars into place will require political leadership and adequate management of intelligence organizations. Political leaders can enact intelligence laws attuned to the present environment. Such laws disassociate intelligence activity from repressive state behavior, and establish adequate mechanisms for democratic control and respect for individual rights and liberties. Intelligence organizations can impose deep changes to their organizational frameworks, operational doctrine, and professional preparation of personnel. They can also improve their association with other parts of the society, especially the academic sector.

Author's Biography

Mariano Bartolome holds a doctorate in international relations from Argentina's *Universidad del Salvador* (USAL), with postdoctoral work in international security for the National Council of Scientific and Technical Research (CONICET). He also earned a master's degree in sociology from the Science Academy of the Czech Republic. He serves as a professor at USAL, the *Universidad de Buenos Aires*, and the *Universidad Nacional de Lanús*. Additionally, he serves as graduate director of public security policy at the *Universidad de Morón*. **Email**: *marianobartolome@yahoo.com.ar*.

Economic Intelligence: An Examination of Its Status in the Andean Countries

Alvaro Jose Venegas Gonzalez

"Among Western countries the fight against global terrorism will increasingly need to be carried out on economic terrain. This is one of the areas that requires greater state intervention and a reduced role of the market and of political actors with vested interests."

—George Magnus, Senior Economist, Swiss Bank Corporation (UBS)

"A prudent man sees danger and takes refuge, but the simple keep going and suffer for it."

—Proverbs 22.3

The Proposal

This essay proposes to enlarge the strategic scope of intelligence. It will show how this government function can address the contending economic interests at play in a country's internal and external security environment. The essay argues that strategic intelligence should discern or anticipate economic challenges to the state and allow it to survive and perhaps prosper in the international system. To illustrate how economic challenges may unfold, the essay documents one Andean country's use of its energy resources, ideological infrastructure, and illicit commerce to impact the security of its neighbors. The author employs the Theory of Adaptive Realism to examine how the intelligence process can bring a strategic economic perspective to public decisionmakers at the highest level.[363]

The Scenario

As the international economic context has changed, governments in the region have become vulnerable to challenges from above and below.

> If bankers and international finance are eating away at states from above, terrorists and drug traffickers challenge state power from below. They make use of technology and of international networks to act around and through states,

> pursuing their objectives by trying to compel states to acquiesce or by eluding the control of states.[364]

More than two decades ago, Carlos Lleras Restrepo, economist and ex-President of Colombia, pointed out that "[a]s bad as are the terrorist attacks, even worse are the [unremarked] attacks on private and public assets."[365] Given this warning, one wonders how this country could not have been prepared to prevent the long-running scourge of attacks on economic targets.

The economist Moises Naim, originally from Colombia, affirms that market reforms of the 1990s debilitated government control of borders.[366] The reforms also incentivized criminal organizations (pseudo-companies) to erode national economies through illicit markets in arms, drugs, human beings, intellectual property, and money. The weak efforts by states to anticipate the intentions and actions of these nonstate actors allows them to operate in a gray zone between legal and illegal transactions.

Presently, governmental intelligence and counterintelligence agencies do not have the capacity to undertake the collection, analysis, and transmission of actionable economic information. Should the private sector, which enjoys the freedom of action to address this problem from a specialized and dynamic perspective, perform this function? The author does not believe so. If private intelligence were to acquire privileged economic information from countries with which there exist political differences, then one could imagine a conflict of interests. In the absence of clear legal boundaries and state regulation, it would seem difficult for private consultants and investigators to resist using that information for the benefit of their own interests.

Further, any private counterintelligence activity that reduces the capability of a competing foreign intelligence service can give rise to a conflict between countries and even armed conflict, thereby unduly affecting the entire home country.

A Spanish author qualifies these points:

> [I]n relation to those functions that are considered "inherently governmental," although it has to be admitted as a general rule that private enterprises should not engage in the

> [intelligence] function, in practice, recourse to the private sector may become necessary in some cases.[367]

Intelligence should be a competitive tool that protects national interests in times of either shortage or abundance. Economic security benefits from development and growth, with healthy labor unions and socially responsible corporations. Private and corporate influence on government policies should not detract from the state's ability to promote the common welfare.

Government-based civilian intelligence specialists in international economics, business, and finance can bring practical and revealing results. They can unite open sources of information with the product of intelligence collection, transmission, anticipation, and the degradation of opponents' efforts (counterintelligence), as envisioned by the theory of adaptive realism.

Taking all this into account, what should be the objective and methods of a working group within the government bureaucracy that intends to achieve the goals of strategic economic intelligence?

Background to a Theoretical Perspective

Definition of Strategic Economic Intelligence

Knowledge from collecting, compiling, evaluating, disseminating, and protecting available economic information creates strategic intelligence. Economic information pertains to national or international phenomena that present a challenge or an opportunity for the promotion or protection of national interests. It remains distinct from economic espionage, or "clandestine and illegal activity carried out by a foreign government and/or a private company to access privileged information about the economy of a country, for the purpose of obtaining an economic advantage."[368]

The region requires legislative initiatives to establish penal codes for economic crimes. Official documentation of illegal economic activity remains uncommon but necessary to spur legislative action. As noted by a Peruvian observer, "Economic crimes here are not accorded social rejection as in Europe, and therefore penal law for economic criminals does not exist here."[369] If lawbreakers in the economic realm were labeled as a type of "enemy," or a source

of danger to be neutralized in any way possible, then they would become legitimate intelligence targets.

In economic terms, intelligence seeks to point out areas of weaknesses in the protection and maintenance of a state's production capacities, employment, and development policies. It also aims to promote the survival of the state in the international system. Thus, intelligence supports economic policy implementation by learning the intentions of international economic competitors; analyzing economic tendencies and negotiations; and advising politicians on the "rules of the economic game" (bribes, lobbying, boycotts, blockades, embargoes) as practiced by competitors.

Principles of Strategic Economic Intelligence

Government knowledge of economic activity in the Andean countries, including aspects of business and finance, remains inadequate. An exception is Venezuela. As the late Venezuelan President Hugo Chavez noted, The Directorate of Intelligence and Preventive Services, now the Bolivarian National Intelligence Service, in the past

> was a repressive, contentious body. Its officials were out in the streets on motorcycles, shaking people down, threatening them, but the new agency is there to conduct economic intelligence, on an international level—state intelligence.[370]

Ecuador, another country if the region, has a limited capability to undertake financial intelligence operations. It can do little to prevent or detect or prevent the laundering of assets or the financing of terrorism. It has neither a state policy nor a strategic plan to prevent money laundering and to combat the financing of terrorism. In 2010, the international Financial Action Task Force blacklisted Ecuador for its lack of money-laundering laws.[371]

Academics and practitioners have written little about the nature and purpose of strategic economic intelligence. However, a few Spanish academics have addressed their country's economic intelligence scene. According to this literature, economic intelligence focuses on how the management of clandestine and confidential human resources affects national economic security. This approach stands in contrast to the nature of economic intelligence envisioned by the present paper. In the Andean region, economic intelligence would

rely on a system for observing, monitoring, and exploiting open sources, like "business intelligence." Business intelligence often seeks out foreign sources, and takes advantage of information obtained by means of espionage carried out by the secret services of the state.[372]

Despite economic reforms that have accompanied market liberalization in the Andean region, and the correspondingly greater exposure to international rivals, economic intelligence capabilities have lagged. For the Spanish, as well as for the Andean region, addressing the applied problem of strategic economic intelligence will benefit from combining two approaches: one representing the public interest—which is intelligence—and the other representing the private world—the discipline of economics.

Intelligence and Economics: How May Their Practitioners Become More Alike?

The work and the interests of an intelligence practitioner and an economist usually appear very different and incompatible. Citizens tend to understand the work of an economist, who deals with public data and generally enjoys public and social recognition. In addition,

> [A]t first glance, economists and intelligence analysts seem to operate in separate spheres, one dealing with economic problems, the other investigating security matters. The economist works with overt data, while the intelligence analyst's data may be secret. The economists' estimations are based on quantitative and formal methods, while the intelligence analyst often makes assessments based on speculation and "gut feelings or instinct."[373]

The professional behavior and capability of economists seems to rest on the ample theoretical development of their academic discipline. That is, any economist can support a policy argument by referencing the results of experiments in public policy (using public data resulting from economic policies put in place at some time in the past), thereby contributing to economic theory and its ethical application.

On the other hand, the specialist in intelligence sets out a less legitimate point of view because data have necessarily been less examined, personal experience

guides assessments, and individual practitioners typically produce inferences from incoherent and sparse data points.

Few government employees in Colombia, whether economists or intelligence analysts, enjoy prestigious educational backgrounds, use leading-edge technology, have systematic knowledge, or exhibit a tendency to follow suitable protocols. Economists, in particular, need sophisticated training and education:

> Those who hold only a bachelor's degree in economics are not employed to diagnose and treat the main "economic ills" of the country…. To reach the level needed for such employment, one must acquire advanced degrees, and preferably a Ph.D. in the United States…. What we do know is that economics departments in universities are proliferating, and producing more graduates who are not prepared to work in decisionmaking centers.[374]

This factor promotes a "culture" of using intuition over reason, a less than ideal basis for contributing to the decisionmaking process.

Qualified economists can base their assessments on well-documented, theoretically sound procedures. Intelligence analysts typically cannot do so. Would the application of a theory of intelligence to the problems of economic competition in the Andean Area improve the professional capacity and credibility of a strategic economic intelligence team?

Theoretical Application—Sims's Theory of Adaptive Realism

The responsibility to confront international opponents is not a new government function and intelligence exists to guide the effort. Jennifer Sims understands intelligence as the useful knowledge resulting from the collection of information, its analysis and its dissemination in support of the cause of decisionmakers, leading to advantageous decisions with respect to their rivals.[375] Sims's theory offers the best available approach to support the present investigation. The theory identifies four critical functions: collection, transmission, anticipation, and manipulation (the last to influence and damage the opponent's intelligence capabilities).[376] It offers the systematic and measurable

means to evaluate success in economic intelligence activities, as illustrated below in two Colombian case studies.

Empirical Vision: Strategic Economic Intelligence in the Colombian Political Decisionmaking Process

Case Study 1: External Security

Background: the Venezuelan parastatal—PDVSA—showed interest in buying the Colombian gas company Ecogas and its network for distributing 45 percent of the country's natural gas. PDVSA also showed interest in owning the refinery in the port city of Cartagena. These moves logically complemented the gas and crude oil pipeline that PDVSA hoped to construct through Colombia to transport fuels from Venezuela to Panama, according to the ex-President of PDVSA, Luis Giusti.[377]

These developments worried Colombian subject-matter experts and political leaders. It could mean surrendering control of this strategic economic sector to Hugo Chavez's political objectives. Because of the highly charged ideological environment, Chavez was making use of the strategic weapon of oil diplomacy to develop the Bolivarian Revolution and fortify his leadership in Hispanic America.[378]

> According to [Juan Manuel] Santos [ex-minister of defense and today President of Colombia], the intentions of the Venezuelan President, Hugo Chavez, to invest in the petroleum sector and in Colombian gas can be "dangerous" because more than an economic interest, a political motivation is perceived … natural gas benefits thousands of Colombian users and in the case of some political contretemps with Chavez, he could simply turn off the "key" to the provision of fuel and bring harm to the nation.[379]

In addition, PDVSA activity extended beyond economic activity to affect foreign policy, international economic relations, external alliances, and national defense policies from a markedly anti-imperialist perspective. PDVSA acquisitions spearheaded Venezuela's execution of an aligned security and defense policy that would involve its armed forces.[380]

These potentially alarming developments masked an even larger problem. Colombian police see illicit border commerce as mere "contraband," and its perpetrators as simple "criminals."[381] Borders create opportunities for smuggling rings, allow global networks to damage a national economy, corrupt the police, and undermine institutions.[382] Border controls might be iron-clad, but illicit commerce in goods, services, and manpower will still exist on one side of the border because some public servants in key positions will allow it to continue. They will decide to defend the lucrative illicit commerce of the criminal networks rather than enforce controls. New centers of criminal, economic power emerge as a result. One center occupies the border area between Venezuela and Colombia:

> There is a lot of illegal contraband along the frontier between Colombia and Venezuela that involves drugs, gasoline, and automobiles. Even though the Triple-Frontier region where Brazil, Paraguay and Argentina come together is better known as a Latin American center for contraband, the border between Colombia and Venezuela is perhaps even more porous and sees vast quantities of cocaine and other basic products … and even if they [criminal groups] do not have a national agenda like the AUC [United Self-Defense Forces of Colombia], they understand that their power grows and criminal enterprises prosper whenever they have good connections with local political leaders.[383]

Intelligence evaluation: The authoritarian Chavez focused his agents' attention on economic forces, natural resources, and the process of industrialization and international trade in Colombia. The knowledge he obtained could forge an economic weapon for potential "warfare," given that strategic surprise can occur in the economic sphere as well as the military realm.

The French economist Frederic Bastiat describes the scenario where illicit border commerce has operated for years: "When merchandise is not allowed to cross borders, soldiers will" or "if cotton, sugar and rice can cross borders, then terrorists may not be able to do so."[384] Strategic planners understand these maxims, which were seen when Venezuela restricted business with Colombia and at the same time strengthened its military apparatus along the boundary as a dissuasive force to affect the choices of the weaker state.[385]

The decision process: Colombia and Venezuela have for some time experienced strained economic and commercial relations. In this environment, civil officials, private consultants, and commercial development funds saw value in gathering relevant information and impressions from foreign diplomats. Their aim was to identify strategic sectors at risk of being acquired or of being interfered with by the Venezuelan government.[386] Colombian government and private officials sought to use intelligence practitioners to collect data and anticipate how political actions may affect investments, capital funds, and foreign trade.

Intelligence officials who use information to anticipate and contain the intentions of opponents act in accord with the premises of adaptive realism. Among Colombian civil servants and industrialists who occupy positions of political and economic leadership, most have little experience in the world of intelligence. Still, the purpose of intelligence in business, politics, or sports is well understood: to secretly obtain advantageous data on an opponent's plans, capabilities, behavior, and the relevant context.[387]

Unquestionably, politically powerful officials should be able to make choices and produce decisions quickly and confidently. The value and the knowledge of strategic intelligence officers, their anticipatory function, and the nature of problems best addressed by state intelligence all remain less certain. A poor understanding of intelligence contributes to high levels of uncertainly among political leaders as they make decisions about its management. Naturally, they hesitate to accept input to their decisions from those whose knowledge may be deeper than their own. To do so would be to admit what they do not know, or acknowledge how little they do know.

Case Study 2: Internal Security

Background: Harm came to a large number of Colombian citizens in 2008 when they mistakenly placed confidence in money schemes (pyramids) offered in southern departments of the country (Cauca, Nariño, and Putumayo). Illicit practices had boosted the economic power of drug trafficking there, and the Uribe administration declared a state of social emergency. The declaration of emergency permitted more thorough investigations and stiffened penalties for such practices. The government aimed to recover and refund money and improve the business climate in the affected regions.

> **Compatriots**: The crime of massive and illegal acquisition of money, by whatever means, whatever the fiction behind which it hides, is a crime against the economic and social order, and generates deep social disturbances ... and generally missing money means robbery, because these organizations are not monitored by official institutions, and in addition do not satisfy the requirements of the law, and it all amounts to a serious social disturbance.[388]

Colombian authorities knew that one FARC (Revolutionary Armed Forces of Colombia) front engaged in illegal financial activities, even though the organization's overall leaders disapproved:

> Although the story varies, authorities have been revealing in recent days the contents of what appears to be the computer of "Edgar Tovar," head of front 48 of the FARC, who is wanted for breaking the law in Putumayo. As everyone knows, David Murcia Guzman, the brains of [the holding company] DMG, had its epicenter in Puerto Asis and it was from there that it began to expand its business.… Police report that the computer, found during Operation Strength, which took place this past 20th of January, held the list of sanctions from the secretariat of the FARC against this group for having invested 15 thousand dollars (about 30 million pesos) in DMG, without the authorization of what they call the General Staff.[389]

Evaluation of intelligence: The illegal practices of these "businessmen" placed state security at risk because of the large number of people affected. Public perceptions of fraudulent investment opportunities led to increased insecurity and lawlessness.

> The governor of Putumayo, Felipe Guzman, alleged to President Alvaro Uribe that the FARC would be taking advantage of the discontent felt by people because of the pyramid schemes, and would set them against the government. Guzman reported that since this past Sunday the FARC has used explosives, has intimidated farmers, and

> has distributed pamphlets to influence the inhabitants of the regions most affected by the pyramid schemes.[390]

The image of the Colombian government suffered more when Eduardo Sarmiento, dean of the economics department of the Colombian School of Engineering, informed the press that the government "was entangled" in a semantic discussion of whether they were pyramid schemes, "when what they needed to do was simply to check account balances, to recognize that liabilities exceeded assets and that there was great risk."[391]

The decision process: The government did not have clear knowledge of the situation as a result of unclear data, information, evidence, and assessments. The intelligence services did not assess the full implications of the fraudulent economic activity because of its relatively arcane, specialized nature. The ex-Minister of Revenue Juan Camilo Restrepo declared, "I believe that there was unwarranted delay on the part of the Government in taking preventive measures. The problem of the pyramid schemes was there to be noticed for more than a year, or year and a half."[392]

The absence of clear strategic economic intelligence assessments for national decisionmakers prevented political leaders from reaching an early understanding of the situation. As a result, they failed to make the timely decisions that could have prevented political embarrassment.

Bringing Doctrine to Strategic Economic Intelligence: Applying the Critical Functions of Adaptive Realism

A casual observer may conclude that criminal threats to national economies cannot be eliminated or readily reduced. However, practitioners realize that a combination of preventive intelligence and counterintelligence actions can diminish potential crimes in the economic sphere, as these crimes often take place in the gray area between legal and illegal activity. Pertinent, anticipatory information contributes to bringing better administrative or penal decisions to the fight. This part of the essay outlines how a strategic economic intelligence unit might address a government's need for timely assessments.

The first Colombian case study cautions us to weigh the potential effect of economic intelligence activity on the country's relations with its Andean

neighbors. Overzealous actions could undermine mutual confidence or paralyze diplomatic efforts and endanger economic relations. Some Andean countries have enough economic and political differences so that a single, intelligence-related misstep could bring on active hostilities.

This base of understanding permits the systematic implementation of Sim's four critical intelligence functions to 1) internal finance and 2) international trade. Intelligence and counterintelligence cannot cover problems that might arise along the entire economic spectrum; comprehensive coverage remains an unrealistic expectation because of the magnitude and diversity of national economies.

Information about some of the Andean countries will not be available to an economic intelligence team because of its confidential or secret nature. Incomplete information makes this essay realistic in reproducing the analytic environment familiar to intelligence professionals. It should also bring realism to the illustrative application of Sims's theory to the work of strategic economic intelligence.

Collection of Information

In accordance with Sims's thinking, strategic economic intelligence must count not only on open sources of information, but also on human-resource intelligence. Through diplomatic legations, commercial representations, and public and private companies, a select group of reliable and experienced intelligence agents would gain access—by espionage, if necessary—to economic, commercial, and financial data using the full range of methods and sources of intelligence. An independent economic intelligence team would attract economists and commercial experts as well as commercial and international finance specialists. Team members would build familiarity with economically influential institutions and international power brokers and gain access to internal circles. Access to these key players would allow the intelligence team to obtain, process, and disseminate data on targets of interest. The Colombian newsmagazine *Semana* characterizes the typical intelligence specialist:

> The majority of secret agents are quiet and discrete, able to infiltrate high diplomatic, governmental or business circles without creating a lot of suspicion. Under the protection of

> covers that range from exchange students to industrialists, from tourists to employees of multinational enterprises, the great majority would not use a weapon to secure their objectives. To the contrary, one of them declared to *Semana* that his mission more resembles being a data processor dedicated to compiling valuable information, processing it, and then giving it to his government.[393]

A concrete example of human-source intelligence collection on economic issues appeared in the newspaper *El Espectador*:

> The indicted ex-Director of Intelligence Fernando Tabares reported new details to the court. He claimed that the Embassy of Venezuela in Colombia had 80 civil servants who were intelligence agents for the Chavez government, and that the DAS [Administrative Department of Security] had discovered their orders from the Venezuelan Directorate of Intelligence [DISIP]. In this way, we discovered that some economic entities, the military, and even Colombian politicians were penetrated.[394]

This evidence shows how counterintelligence activity can contribute to gathering economic intelligence in areas vital to national security. Economic intelligence in this case emerges as a byproduct of the continuous observation of Venezuelan intelligence activity in Colombia. Venezuela can undertake wide-ranging intelligence operations and therefore potentially outmaneuver its rivals because of the financial power accruing from its oil industry.

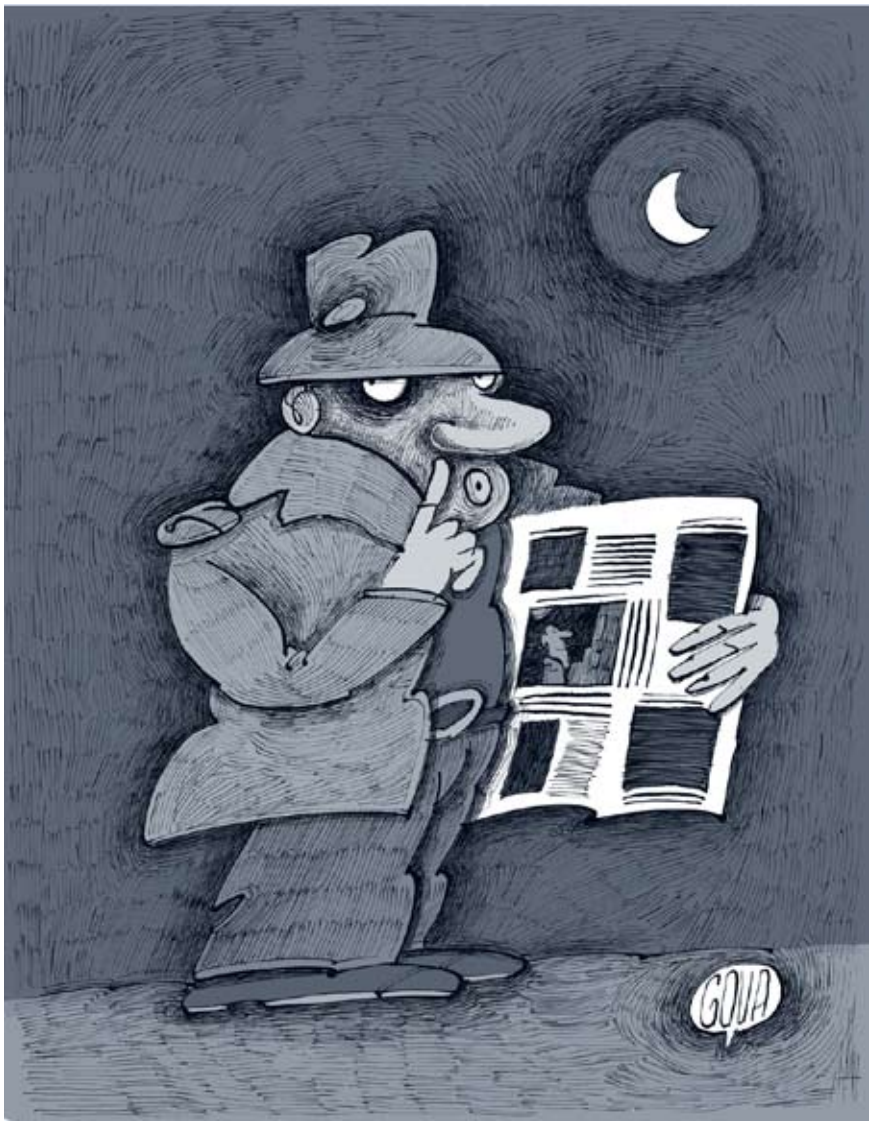


Figure 6. Wow! Enough risk for today. Also enough for tomorrow.
Source: courtesy of Andres Gonzalez.

Anticipation

Economic intelligence practitioners accomplish anticipation in two ways. First, their collection of information needs to remain independent of the preferences of or the preapproval of political officials. Second, they need to develop an ability to warn intelligence customers about unexpected competitors or new adversaries.[395]

To determine how well intelligence specialists perform the anticipatory function, one needs to evaluate whether they have risked going beyond the usual "current intelligence" approach. Have their assessments sometimes disagreed with the view held by decisionmakers, even though consistent with their policy objectives? The specialists' role is to identify new adversaries and alert political officials to the threat they may pose to the country's business and finance communities or its international economic relationships. At the same time, intelligence specialists need to protect sources and methods of intelligence in order to reduce their own vulnerabilities. Effective specialists in strategic economic intelligence anticipate the challenges and opportunities that political decisionmakers often ignore. Their alerts also extend to those who might be excluded from the policymaker's closest circle of economic advisors.

Some of the difficulties highlighted in the case studies resulted from the actions of other countries; others originated from unwise remarks by influential domestic actors. Thus, Colombia did not anticipate the commercial crisis with Venezuela in part because of Venezuela's actions with respect to foreign exchange. Acting in their own interest, the Venezuelans brought some Colombian exporters to the brink of insolvency by delaying delivery of payments.[396] Likewise, trade union leaders of ANALDEX (Colombia's National Association of International Commerce) and ANDI (National Association of Colombian Businessmen) made imprudent remarks about the coup d'etat that temporarily removed Chavez from power in April 2002. Their comments later led to some Colombian companies' being denied permission to establish operations in Venezuela.[397]

Additionally, after the Colombian Army swooped down on FARC leader Raul Reyes in Ecuadorian territory, relations between Colombia and Ecuador deteriorated. The Ecuadorian government decided to impose foreign-exchange safeguards against Colombia in July 2009 as part of its monetary policy.[398] In

this way, Colombian commercial exchanges began to be affected by international political developments. If Colombia had discrete emissaries who could have obtained data to anticipate these events, the security of Colombia and its commercial interests in Venezuela and Ecuador may not have been placed at risk.

As a result of their having to address multiple problems simultaneously, high-level decisionmakers naturally resist uninvited changes to their policy agenda. Decisionmakers may reject new information that is not consistent with their priorities as a result of a parochial vision of the world, or in the case of economic intelligence, because of competing private interests.

Transmission

Once an adversary and its capabilities are identified, the question becomes to whom and how to transmit that information. Communication requires confidence between the intelligence service and the decisionmaker. A measure of that confidence lies in the ability of the intelligence service to deliver valuable information with utility for decisionmaking.

When intelligence maintains independence from a decisionmaker, rival sources of information may emerge and the transmission of intelligence can decay or fail. Excessive closeness or friendliness with the decisionmaker may lead to overlooking or accepting his or her errors. For that reason, Venezuelan President Chavez used two intelligence services (domestic and Cuban) to arm himself in the event of a break in the relationship with one of the two agencies. Having two agencies at his disposal also extended his vision and hearing, giving him time to act and avoid errors.[399] Cuban interference in Venezuelan internal affairs led to considerable resentment even among Chavez supporters. According to Americo Martin, former guerrilla and Venezuelan politician,

> [a]t this time, Cuban activity is multiplying in the military environment, as well as in intelligence and counterintelligence. It is a powerful, ideological penetration. Members of militia groups, professional military personnel, and hundreds of leaders are being trained in Cuba.… Chavez sees dissidents as enemies, or at the least, he blames them for the assassination of public figures and coup planning. He has

> no confidence in his followers, requires absolute loyalty, and only feels secure when surrounded by Fidel's emissaries.[400]

Like Chavez, any decisionmaker has the opportunity to gather intelligence from competing sources. In the civilian world, this information often comes from powerful people rather than from public opinion. Still, any decisionmaker will want to extend his eyes and ears through an intelligence service that evaluates the data collected in his name. Intelligence services remain subject to mechanisms of accountability and monitoring that guarantee loyalty to a cause and to policy. This perspective received attention in a Caracas newspaper, with intended irony:

> When I say a people without a memory, I mean that Venezuelans forget the bilateral accord with Havana that permits Cuban state security police personnel to undertake police work and espionage in Venezuela. When I say ungrateful people, I mean the lack of gratitude by Venezuelans for the control exercised by the Cuban Security Department (G2), for their intelligence services, for identification and immigration services, for public registry and notary services, all of which look out for the citizen, his identity, personal documents and property.[401]

This commentary illustrates that a political leader's security perspective (Chavez's support for Cuban intelligence operators in Venezuela) was not shared by citizens at large. Indeed, a trusted confidant would prove his or her worth to a political leader by transmitting an alert about the open but creatively masked dissent of opponents.

Figure 7. Is that the truth, the whole truth, and nothing but the truth?
Source: courtesy of Andres Gonzalez.

Counterintelligence

In a globalized and competitive world, countries can readily justify engaging in unlawful espionage. Similarly, they employ counterintelligence measures to reduce the efficiency of opponents' intelligence services. Simply put, counterintelligence exists as a response to intelligence activity.

Adaptive realism suggests that where security interests face off against one another, there are two ways to make an advantageous decision. One is by collecting the best information on the activities of the adversary; the other is by distorting the opponent's information while protecting one's own information (counterintelligence). The latter approach has two components, defensive and offensive, as indicated in the table.

Table 8 Two Components of Counterintelligence	
COUNTERINTELLIGENCE	Defensive: Information protection achieved for one service by blocking information collection by another service.
	Passive form (preventive): includes the use of stakeouts and surveillance, safehouses, deserters, interrogations, spies, etc.
	Active form (operative): attracts the attention of spies, provokes and deceives the hostile service, forces revelation of hostile methods using distractive decoys. With this approach one looks to demonstrate a totally hostile approach to suspicious individuals or organizations.
	Offensive: Its purpose is not to block the operations of the opponent, but to change or to break the intentions of the adversary by playing with his mind. It defends one's own operations and distorts the information gained by the opponent. Also, it obtains advantages for oneself through mechanisms that allow the manipulation or the biasing of the intelligence capabilities of the other side, impacting its activity and its prospects for survival.
	Passive form (preventive): involves deceptive practices or camouflage; features people with fake titles or people with an interest in establishing empathy or "friendship" that has as its hidden aim obtaining sensitive information.
	Active form (operative): uses double agents and deception. That is, an agent leads the adversary to false judgments through double agents. Disinformation hides specific activities, such as the information interests and intentions of one's own service, and deflects the attention of an opponent's espionage toward other targets of lesser value.

Source: Compiled by the author.

Two counterintelligence examples involve Venezuelan intelligence activities in Colombia. In the first, the subject of interest was a military intelligence practitioner.

> Jose Gregorio "Cheo" Guzman arrived in Colombia in 2003 as an official of the embassy of Venezuela, with the supposed job of facilitating business between entrepreneurs of both countries. Although his position was not at the highest rank, within a short time entrepreneurs and politicians realized that this was Chavez's man in Bogota. Known as a zealous member of the Motherland for All party in Venezuela, he was also known for being very near [Chavez's] Miraflores Palace, although he maintained a low profile.[402]

The idea that "in just a short time industrialists and politicians realized that this was Chavez's man in Bogota" set the stage for "defensive-active" counterintelligence activity by the Colombian side.

The second example of Colombian defensive counterintelligence activity involves irregular economic behavior in support of the Chavista expansionist policy. This evidence emerged as a result of the pressures brought by envoys of the Bolivarian government, who had explicit orders to use the private resources of the business known as *Monómeros Colombo Venezolanos* to finance people and organizations supporting the Bolivarian movement in Colombia.[403]

In the purely internal security realm, an example of active and passive, offensive counterintelligence comes from the experiences and testimony of a sergeant major of the Colombian Army of Colombia. His exploits occurred in the 1960s. Working undercover and adopting fictitious identifies, deceit, manipulation, and other mechanisms, he influenced the will, information, and actions of rural brigands. These criminals, like others now, strengthened their finances through extortion and "taxes," accompanied by the support of wealthy proprietors or politicians of note in the provinces.[404]

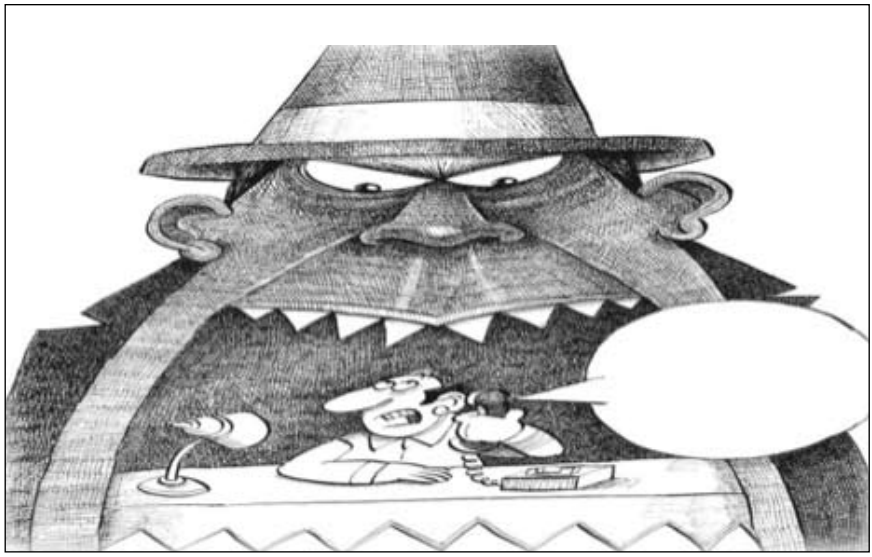


Figure 8. Hi boss, this time I think there's some news.
Source: courtesy of Andres Gonzalez.

Summary

The effective operation of a strategic economic intelligence team depends on public officials' ability to recognize and leverage the functions of intelligence. To that end, Colombian national Law 195, article 4, Part C, declares that intelligence and counterintelligence information can be obtained for the purpose of protecting natural resources and the economic interests of the nation, a finding that recognizes the role of intelligence agencies in protecting investments, commerce, economic development, and therefore national economic security.[405]

As illustrated by the foregoing examples, systematic application of the principles of intelligence and counterintelligence by the secret services and other organizations responsible for monitoring economic phenomena may lead to recognizing threats and opportunities and safeguarding national security. Table 9 distills some guidelines for the management of an economic arm within the intelligence services with the objective of fortifying an intelligence community.

Table 9
Guidelines for Collaborative Action by a Strategic Economic Intelligence Team

Sims's Functions	Economic Intelligence Team Activity	Participating Organizations
Collection of Information	Identify key economic actors, their reputation, their investments and capacities. (Financial situation, expansion plans, and extent of international economic and commercial relations.)	National Planning Office Revenue and Banking (Office of Financial Information and Analysis and Directorate of Taxation and Customs)
	Have the sourcing of estimates, analysis, and investigative reports reviewed by academics and private and public consultants who are active on the economic scene.	Ministry of Commerce, Industry and Tourism Ministry of International Relations
	Collect and compile information related to the insertion of illegal armed groups and corrupting agents active in economic circles.	Ministry of Mines and Energy Trade Unions – National Council of Trade Unions and Chambers of Commerce
	Monitor national and international economies through the Web and specialized subscriptions.	
Anticipation	Anticipate illegal exchanges through black markets and opportunities for corruption. Work with experienced professionals who can assess risks to national economic interests operating outside the country.	National Planning Office Revenue and Banking (Office of Financial Information and Analysis and Directorate of Taxation and Customs) Ministry of International Relations

Table 9
Guidelines for Collaborative Action by a Strategic Economic Intelligence Team (continued)

Sims's Functions	Economic Intelligence Team Activity	Participating Organizations
Transmission	Make risk assessments and threat warnings available to key players in the national economy as well as to international business and finance entities.	National Planning Office Trade Unions – National Council of Trade Unions and Chambers of Commerce
Counterintelligence	Neutralize intelligence operations of hostile actors that threaten the strategic infrastructure and national economic security. Watch over urban and rural areas where there are projects underway with high environmental and land value impacts. Operate in areas where there is no open information and where the private sector cannot operate. Address special information requirements.	Revenue and Banking (Office of Financial Information and Analysis and Directorate of Taxation and Customs) Ministry of Commerce, Industry and Tourism Ministry of Agriculture

Source: Compiled by the author.

Strategic Economic Intelligence and the National Intelligence Community

Economic development provides the essential foundation for achieving national security objectives. Strategic economic intelligence teams aim to dismantle the support structures of those who operate outside of the law and anticipate attacks against critical economic infrastructure. Engagement with terrorist activity occurs primarily at the operational level. However, terrorism in Colombia combines all forms of fighting and employs economic warfare to attack strategic economic infrastructure (dams, pipelines, highways, airports, electrical transmission systems, etc.). This targeting by illegal groups requires cooperation between governments and investors to protect the interests of all parties. The protection of oil pipelines in Colombia offers an example of how economic intelligence can mesh with internal and external strategic interests.[406]

Colombia does already have one economic intelligence institution with a strategic focus. The Egmont Group has since 1995 coordinated the establishment of Financial Intelligence Units (FIUs) in various countries. The Colombian Financial Information and Analysis Unit (UIAF) exchanges information with the other FIUs to fight money-laundering crimes and the financing of terrorism.[407] The UIAF, as part of the Colombian intelligence community, operates as an intelligence and counterintelligence unit at the operational level, but within an international, strategic framework. It detects and prevents the laundering of assets and the financing of terrorism through centralization, systematization, and analysis of information. Its personnel are both well-educated and specialized: 77.6 percent work as professionals, and 54.7 percent have undertaken advanced study at the master's level.[408]

Accomplishing the work of strategic economic intelligence in an information society depends on building alliances with private business to gain access to the information required by the UIAF. This approach makes the monitoring and pursuit of suspicious activities an inevitable part of the healthy growth of the state and the economy, rather than its being seen as a conspiratorial practice.

Illicit commerce in Colombia has maintained a constant presence through the history of the country. A 2011 law directs the intelligence community to

combat the problem.[409] the National Directorate of Taxation and Customs (DIAN) must exchange information with the Regional Office of Intelligence Liaison (RILO). RILO operates as a worldwide customs network to handle data on illicit economic activity.

On the other hand, Colombia lacks appropriate political and legal tools to monitor illegal aspects of economic activity more comprehensively. A *Conpes* (National Social and Economic Policy Council) initiative,[410] inserted into the National Development Plan and titled "The Communal State: Development for 2006–2010,"[411] attempted to consolidate gains made in public security. The Conpes document does not address civilian intelligence institutions because of the persistently poor internal practices exhibited by DAS. A new approach to the role of intelligence and counterintelligence in Colombian public security may soon appear in the National Development Plan.[412]

Disciplinary differences between economics and intelligence make it difficult for intelligence to interpret, in advance and with accuracy, a variety of economic phenomena that impact national security. To combat this problem requires the creation of a specialized analytic unit that collaborates with the intelligence community.[413] Appropriate analytic training can foster a better understanding of weaknesses in current efforts by economic analysts, businesses, and financiers who engage in the comparative and systematic analysis of information. Brighter lights can illuminate the obscure realm between legal and illegal commerce where terrorist networks, organized crime, and corrupt public and private entities now operate with impunity.[414]

As economic intelligence gains legitimacy as a contributor to government action and international relations decisionmaking, knowledge-based collaboration between economists and intelligence analysts can positively contribute to the generation of effective public policies.

A Strategy to Broaden the Horizon of National Intelligence

Everyone, it appears, now agrees that the methods of commerce are displacing military methods—with disposable capital in lieu of firepower, civilian innovation in lieu of military-technical advancement, and market penetration in lieu of garrisons and bases.

—Edward Luttwak[415]

If a state exists to protect the life and property of its citizens, then actions taken to prevent damage to national economic interests, even before the true nature of a potential threat is known, have validity. The broad and continuing economic warfare described by Luttwak affects more than tangible interests; it affects the daily life of citizens. Still, the state must balance a concern for security with respect for civil liberties and human rights. How can a strategic economic intelligence team adjust itself to this revised paradigm?

It can begin by taking note of the perceptions of intelligence held among those outside the state establishment. For example, an official of Colombia's Ideas for Peace Foundation suggests that,

> [i]n the middle of the DAS scandals, it has gone unnoticed that in spite of recriminations that muddy the debate, the government as well as the opposition agrees on an undeniable reality: "Colombia needs spies.… And everyone also agrees that vital decisions of the State need to be well-informed, and that the process of obtaining data necessarily involves espionage."[416]

His comments support an integrated and collaborative network among agents of the state and of civil society (economic unions, academics). The network would promote formulation, feedback, and peer review of ideas for carrying out the functions of intelligence identified by Sims. The challenge lies in developing a type of strategic economic intelligence team that can create a binding alliance among all these actors. Somewhat surprisingly, building such alliances may be less complex than expected. Extensive ties already appear to

exist between the government and economic actors in formulating foreign policy:

> Both the business and academic sectors are relevant to the decisionmaking process. Members of the first group, one after another, come into play as individual representatives of specific businesses or as representatives of national conglomerates. At times, too, they assert collective interests through unions or Chambers of Commerce. The economic power of these groups allows them to press for certain decisions and policies, both at the national and international levels, although their participation depends on the political winds. In contrast, the academic sector is more diffuse and tends to distrust governmental actions. However, academicians also consider that proposals by the government generally remain rhetorical, without real impact on nongovernmental groups.[417]

The launch of an economic intelligence entity may also spur the creation of similar capabilities among nongovernment organizations. Information and knowledge synergies between the state's offices and civil society may be supplemented by the emergence of competition between private and public economic assessments as a basic element of national security.

Rather than adopting the reactive techniques of monitoring or planning tactical operations, a strategic economic intelligence team needs to build future-oriented warning capabilities. Further, legal collection and dissemination of information needs to extend to private economic circles as well as public organizations. In short, economic intelligence needs to alert both public and private players about the various threats and challenges posed by actors who are opposed to the aims of the state. Finally, analysts must avoid any involvement with local "potentates" and concentrate on developing indisputable professionalism.

Author's Biography

Alvaro Venegas Gonzalez, a Colombian, graduated from the College of Economic and Social Sciences of the *Universidad de La Salle* in Bogota. He practiced the art of intelligence in the now-defunct Administrative Department of Security. He advocates strengthening the incipient national intelligence culture in Colombia. His work has appeared in *Aquimindia*, the journal of the Administrative Department of Security; in *Aainteligencia*, an online Chilean journal; and in *Nova Et Vetera*, Colombia's public administration journal. **Email**: *aljovego@hotmail.com.*

Intelligence Resource Management

Dan Elkins

Other authors in this book have noted the oversight role of national legislatures in exerting budgetary control of intelligence agencies. The capability of legislatures to accomplish oversight rests on the ability of staff advisers and elected officials to understand how the objectives of each agency fit within a national intelligence system. Specialists in resource management in each agency have the obligation to maintain a dialog with subject-matter experts in their agency to prepare appropriate budget plans and proposals for review by the government's funding officials, whether in the executive or legislative branch. Resource management specialists and intelligence professionals can derive real resource management benefits from continuous interaction with colleagues not only within their agency, but also with their counterparts across an entire intelligence community, in the same way as substantive intelligence practitioners benefit from daily interaction with their counterparts as they pursue intelligence targets and plan operations.

The author of this essay has familiarity with the resource management and budgetary processes of the Intelligence Community of the United States. The principles and practices he has observed and applied in the U.S. also suit any country whose intelligence agencies are accountable to citizens and government oversight offices. This essay acknowledges all levels of accountability, as identified in the Goncalves essay: 1) agency—internal to a particular intelligence agency; 2) executive—carried out within the executive branch by non-intelligence entities of the administration and by the department or ministry to which the intelligence agency is subordinated; 3) external—exerted by the judicial branch, by the legislative branch, and/or by an independent entity; and 4) popular—addressing the concerns of individual citizens or civil society organizations. The practices that allow resource management specialists and substantive intelligence professionals to accomplish internal resource management within intelligence agencies are of particular interest here, but the breadth of the intelligence community means that accountability for those practices extends across much of the executive branch.

Three sets of professionals can benefit from reading this essay: 1) practitioners of the resource management processes and practices explained below; 2)

"functional" professionals who conduct or manage intelligence and related activities (collection, analysis, production, security, intelligence training, information management); and 3) intelligence supervisors with broad resource management responsibilities.

Effective and Efficient Use of Resources

The success of an organization's efforts to secure sufficient resources may well depend on its track record in the effective and efficient use of resources already acquired. An organization's resource management office documents requirements and takes the lead in efforts to satisfy them. However, everyone in the organization bears the responsibility to ensure effective and efficient use of resources.

Measuring Effectiveness and Efficiency of Resource Utilization

Definitions. To be *effective*, an organization must make satisfactory progress toward the accomplishment of its goals and objectives. Regardless of the specifics, the primary mission of any intelligence organization is to *satisfy its customers' needs*, that is, to get the *right quantity and quality* of intelligence to *customers* in a *timely, usable* fashion. This is true whether the customers are national-level policymakers, battlefield commanders, planners, or others. To also be *efficient*, an organization must satisfy these customer needs in a *cost-effective, expedient, highly productive* manner, with *minimal waste* of effort or resources. While *effectiveness* is measured by *results achieved, efficiency* is gauged by the *manner in which the results are achieved*. Effectiveness directly impacts mission accomplishment, while efficiency directly impacts the cost of accomplishing that mission.

An organization can be effective, even without efficiency, when ample resourcing prevails. But with tight budgets, few organizations can long tolerate unchecked inefficiency. This situation usually forces the diversion of scarce resources from crucial operations to keep inefficient operation(s) going. Personnel may also work harder than usual, but cannot do so indefinitely.

Measurement criteria. To measure the relationship between available resources and mission accomplishment one may pose a series of questions. The best

questions address effectiveness and efficiency, as well as whether additional resources may resolve obstacles in the way of achieving those goals. With the assumption that the organization under scrutiny performs only intelligence functions, there exists a limited range of possible answers to each question. The meaning of each answer will be explained.

Question 1. Has the organization properly identified its customers? Most organizations would answer in the affirmative. Although an organization may remain unaware of some potential customers, it has to identify at least one valid customer who needs its products and services. Customers need not be policymakers or warfighters (the ultimate consumers of intelligence). Instead, a customer may simply be another intelligence organization with a need for information.

A ***negative response*** to this question raises a *red flag*. Any intelligence organization that has not properly identified its customers will face resource reductions during austere times and may not survive periods of severe retrenchment.

Some readers may argue that an intelligence organization's *mission* remains more important than its customers. They will say that an agency's effectiveness depends solely on whether it accomplishes its mission(s). This is true only to the extent that the original mission remains valid. Policies and priorities of political leaders and military commanders undergo constant change, as do the needs of intelligence consumers. Only to the extent that customers still need the intelligence specified by a mission statement can an organization's effectiveness be measured by mission accomplishment.

> ***Corollary to Question 1***. The need to keep the customer list *up to date* rivals the basic value of knowing the identity of one's customers. This list must reflect continuous changes, as organizations are created, disestablished, renamed, reorganized, or consolidated.

Question 2. Has the organization determined what its customers need? Even without knowing exactly what its customers need, an organization might happen to provide usable intelligence. The organization will more likely waste valuable time, effort, and resources producing intelligence of little or no use to

any customer. By failing to identify a *clear need* for its output, an intelligence organization may render itself vulnerable to reductions or elimination.

> ***Corollary to Question 2***. As with the previous corollary, an *up-to-date list of* each customer's *needs* will prove vital to an effective intelligence operation.

Question 3. Is the organization *satisfying* its customers' needs? This question focuses on effectiveness. Assuming the organization has identified its customers and knows what those customers need, its *effectiveness depends on the degree of success it has in satisfying those needs*. Customer feedback offers the only way to determine how to answer the question. Adjustments based on useful feedback enhance effectiveness.

Question 4. Is the organization satisfying its customers' needs in a *cost-effective* and efficient manner? Although *efficiency* may not matter so much in periods of plentiful resources, it becomes critical as budgets tighten. Differences between effectiveness and efficiency reflect different points of view:

- The *customer judges* the effectiveness of an intelligence organization. The intelligence *organization itself* feels the effects of its *efficiency*. The officials who review and approve the organization's funding proposals are the *ultimate judges* of its efficiency as they evaluate its utilization of resources.

Analyzing the responses. Each of the four questions deals with a specific aspect of an intelligence organization's performance in identifying and satisfying its customers' requirements. One can summarize the implications of positive and negative responses to these questions as follows:

Answers to all four questions ***YES***

- From a resource management perspective, the organization is successful and should occupy a strong competitive position for securing and keep ing the resources it needs.

Answers to Questions 1–3 ***YES***

Answer to Question 4 ***NO***

- The organization's effectiveness is not in question. But in a resource-constrained environment, the organization's lack of efficiency needs remedial action.

Answers to Questions 1 and 2 *YES*

Answers to Questions 3 and 4 *NO*

- This case requires further study. The organization must determine why valid customer requirements have not been met and take remedial action.

Answer to Question 1 *YES*

Answers to Questions 2–4 *NO*

- The organization must work with its customers to develop and maintain the currency of any requirements list. Once that is done, it must assess its capability to meet these needs and the degree of efficiency in doing so.

Answer to Question 1 *NO*

- In not knowing its customers or their needs, the organization suffers a poor competitive posture with respect to securing new resources and keeping what it has.

Factors that can hinder effectiveness and efficiency. If the organization has determined that it knows its customers and their needs, but is unable to satisfy these requirements, an effort must be made to ascertain the underlying causes of this weakness. Although many potential reasons exist for this failing, shortfalls generally result from one of three conditions:

- ***Leadership/managerial shortcomings:*** poor planning, personality conflicts, political infighting, lack of communication, inappropriate or counterproductive policies, inefficient procedures, poor morale, strained employee relations, hostile working environment, etc.

- ***Structural weaknesses:*** unworkable organizational framework, confusing chains of responsibility, cumbersome and inefficient internal operations,

awkward physical layout of facilities, unsafe or physically uncomfortable working conditions, inadequate interface with external entities, etc

- ***Resource deficiencies:*** shortages of operating funds, equipment, or manpower. Whether real or perceived, most organizations cite this condition as the major cause of their inability to meet customer needs.

Overcoming Ineffectiveness and Inefficiency

Seeking remedies. Turning from problems to solutions, not all remedies suggested here can or should involve additional resources. Often, an organization has all the resources it needs to solve its problems, but its leaders either remain unaware of the true nature of these problems or lack the will to to fix them. Some remedies require external advisory or financial assistance.

Leadership or managerial remedies. This type of problem—usually driven by personalities, bureaucracy, or institutional culture—typically requires *internal resolution*. The organization's leaders need to risk making the changes needed. Personnel at all levels must be willing to participate in the change process, whether the remedial steps were mandated through in-house measures or recommended by outside management consultants.

Organizations suffering from leadership and managerial problems often ignore the obvious and insist on seeking solutions through the budget process. However, those who review these organizations' requests for additional funding may well be skeptical that money will solve the problem. In such cases, they will undoubtedly scrutinize the requests carefully and expect to see sound evidence of exactly how additional funds may help resolve the problem.

Remedies for structural problems. Structural problems can be caused by forces that are either internal, external, or a combination of the two. Requests for additional dollar or manpower resources to address internal or external problems gain strength from the establishment and maintainance of an *intelligence architecture* that outlines current and desired capabilities, organizational roles and missions, functional relationships, and other features of an all-inclusive "master plan" for intelligence. Some architectures overlap because they address issues that require cooperation and interaction among multiple organizations, commands, and agencies. By working together to solve problems of common concern, a number of individual organizations can form

symbiotic relationships. They can pool their resources, act as sounding boards for each other's ideas, and share any benefits from these efforts. Community-wide coordination of architectures brings greater efficiency and effectiveness than isolated efforts by each organization.

Budgetary remedies. If an organization determines that its ineffectiveness is truly resource-related, the budget process would be an appropriate avenue for seeking a remedy. Additional dollar and manpower resources could be pursued through programming and budgeting efforts. Dollar resources could also be sought, in the near term, through reprogramming actions or a request for supplemental funding. The organization's resource managers and personnel assigned to the offices suffering the shortfall work together to develop the project description, supporting justification, and funding profile to be included in the proposal. Once the proposal has been finalized and submitted for consideration in the program and budget build process, the resource managers will follow it through the appropriate resource management system. This path will ideally lead all the way to the inclusion of the desired resources in an approved national budget.

In the United States, acquiring resources through the budget process usually requires a minimum of two years. *Alternative sources* of funds require a less time-consuming and less difficult process. Alternative sources include: a) "sweep-up" money made available during the year to cover unfunded requirements (UFRs), b) reprogramming actions that bring in additional resources, and c) supplemental appropriations. Each of the three can provide short-term funding, but none could be expected to resolve a shortfall that requires sustainment over many years. Funds received through the second and third sources generally fill specific requirements that have already been identified by the time the money arrives. The pursuit of resources to satisfy ongoing requirements will be discussed later in this essay.

Budget Proposal Management

Whether an organization is seeking funding for a new requirement or compiling its input for an annual budget submission, required documentation for a single new requirement or for each item in the annual submission will have the same basic components. These components are: a) a clear description of what is needed and how it will be developed and employed, b) why it is

needed and what can happen if the requirement is not met, and c) a resource summary that projects costs over the years needed to satisfy the requirement. An effective proposal will be readily understood by all those who read and review it. The more one understands how to simplify the development and marketing of a funding proposal, the greater the chance for success in acquiring needed resources. Vague and incomplete language can undermine a funding proposal. The following paragraphs outline how to develop a high-quality funding request with all the necessary ingredients.

Tailoring the request to the audience

Project descriptions and justifications must be appropriate for all links in the approval chain through which the proposal travels. The higher the reviewer in the approval chain, the greater the likelihood he or she will lack the background or expertise to understand technical details and specifications (see later material on how to handle this situation). A project involving a tactical military intelligence asset will address different concerns than a more strategic need. The review process typically involves both military and civilian officials. Each group naturally has a different set of backgrounds, expertise, and concerns.

Developing and articulating a concept. A good proposal first identifies exactly what is needed and how the project will fit into an ongoing operation, if and when it is approved and fielded. Anticipating the project's impact on existing workloads, equipment, space, and facilities requires the preparer to engage in two types of thinking: 1) comprehensive and 2) strategic (or programmatic).

Comprehensive thinking. Those who engage in this type of thinking consider the full scope of the need—not just its basic ingredients, but *all resources* required. They consider supplies, equipment, furnishings, services, construction or renovation of facilities, travel, training, etc. Comprehensive thinking also weighs potential trade-offs that can affect costs and project feasibility. Tradeoffs to consider include purchase vs. lease and the use of contractors vs. new manpower (and in the case of new manpower, whether it should be military or civilian). This type of thinking allows the drafter to anticipate anything that could possibly force adjustments to the concept of operations once the project is underway.

Strategic / Programmatic thinking. Here, one considers the mid- and long-term budgetary implications of the need, beyond the initial costs of implementation. Long-term needs include replacements, spares, maintenance, and the recapitalization of major equipment and systems in future budget years. By thinking strategically, one strives to: a) anticipate all costs associated with fielding a capability, b) minimize the likelihood of cost overruns during implementation, and c) ensure that the capability being established will meet or exceed expectations.

Drafting the Proposal

No matter the particular format used by an organization, a funding proposal contains four components: a program description, a justification, an impact statement, and a funding profile.

Program Description. The narrative should begin with a brief list of the *resource categories* to be acquired, such as *manpower* (military billets, civilian positions, and contractor support); *supplies, equipment, furnishings* (mainframe computers, computer workstations, printers, servers, consumable supplies, communications equipment, light tables, and office furniture); *services* (system and software design and development, intelligence collection and analysis, training of personnel, curriculum development, consulting services); *construction or renovation* of facilities; and finally, anything else to be funded through the project, such as travel and per diem expenses, purchase of software licenses, leasing of communications lines, and flight hours for airborne reconnaissance missions. The program description will also indicate the *intended purpose* of each resource. It should be comprehensive yet concise, with an implementation schedule and major milestones. An effective explanation demonstrates programmatic thinking.

The description should avoid technical jargon and overuse of acronyms, be internally consistent, and fit the numbers in the funding profile (to be described below). If technical details might be useful to some in the approval chain, this information should appear in a separate paragraph in the narrative, in an appendix or in an attachment.

Justification. The justification identifies the underlying *mission need* and explains the impact of non-approval. Mission need refers to identifiable goals

and objectives to be supported by the proposed capability, and indicates how the project will respond to higher-level guidance directed at the organization. The body of the justification explains how the project expects to satisfy the mission need. An effective justification convinces reviewers that the project represents the *best of all alternatives* that might be offered to accomplish the mission.

Impact Statement. Whereas the justification explains the adverse impact of not funding the project, an effective impact statement explains its *implications or ramifications* for national security, support to warfighters, or some other high-level concern. The impact statement emphasizes why reviewers should care about those implications. In some instances, the statement may highlight the failure to take advantage of a measurable dollar, manpower, or time savings if the project is not approved.

Funding Profile. This *resource summary* of the project's *financial and manpower costs* appears in a spreadsheet. The top portion shows financial costs by fiscal year and the bottom section indicates manpower figures (in whole numbers of military billets and civilian positions). The example in Table 10 shows resource categories used by the United States Department of Defense.

Table 10
Intelligence Resource Summary Spreadsheet

Categories	FY 2	FY 3	FY 4	FY 5	FY 6
O&M					
Procurement					
RDT&E					
MilCon					
MilPers					
Total Costs					

Officer					
Enlisted					
Civilian					

Table 10 Intelligence Resource Summary Spreadsheet (continued)					
Categories	**FY 2**	**FY 3**	**FY 4**	**FY 5**	**FY 6**
Total Manpower					
O&M=Operation and Maintenance; RDT&E=Research, Development, Test and Evaluation; MilCon=Military Construction; MilPers=Military Personnel.					

Source: Compiled by the author.

An explanation of costs will alert reviewers to the factors behind the figure in each block. Careful explanations of multiple expenditures in the same category may save a proposal from arbitrary reductions, as reviewers can gauge the impact of not funding a particular item.

Marketing the Proposal

Creating a viable funding proposal requires considerable effort. The requester cannot leave the fate of even a clear and properly constructed proposal to chance. The requester needs to "work the system" by arranging as much exposure as possible for it as the larger organization's program and budget are formulated. Only the proposal's originator knows the project's value to the mission and the organization.

Marketing takes place at all organizational levels, as branch supervisors vie for acceptance of their respective project concepts. Division supervisors, in turn, compete to gain favor with higher-level officials as part of the deliberation and decisionmaking process. Some organizations extract facts and figures from written proposals for summary in "quad sheets" or "quad charts" for use at prebriefings, briefings, and decision briefings. These tactics aim to cull the few real gems from disparate, competing proposals, to improve the chances of funding the most deserving projects.

Budget Principles for Supervisors or Office Directors

Resource Responsibilities of Supervisors

Supervisors routinely provide resource managers much of the data and justifications for program and budget build. Whether they realize it or not,

all supervisors in intelligence organizations have certain resource-related responsibilities as described below.

Defending existing resources. The budget process deals not only with the pursuit of future resources, but also the defense of those currently on hand. In periods of declining or flat budgets, the only way to fund anything new is to "take it out of hide." This forces organizations to offer items in the current program-of-record as compensation for later funding of some of the new items proposed in their budgets. Thus, managers must always be prepared to defend their assigned resources to keep them from being used as bill payers. The same preparation will prove useful when they have to provide input to data calls referred to as "what-if drills." In these drills, supervisors show what they expect would happen to their operations if their budgets were cut by some arbitrary figure, such as 5 or 10 percent. A knowledge of the basics of the budget process can be helpful even to those who do not foresee a need to seek additional resources.

Filling unfunded requirements. All organizations strive to obligate as much of their budget as possible each fiscal year to avoid losing unobligated budget authority. This prompts mid-year and end-of-year execution reviews, designed to find any budget authority that will likely not be obligated by the end of the fiscal year. "Excess" money can be "swept up" in these reviews and diverted to unfunded or underfunded projects. Competition for "sweep-up" money generally involves a process similar to the annual program and budget build (though usually on short notice). Those who can quickly produce funding proposals that demonstrate a critical need for resources stand to gain some of this excess money.

Manpower and personnel management. Supervisor responsibilities at various levels of intelligence organizations include manpower resource management. In this role, supervisors: a) periodically identify staffing shortfalls that can be addressed in the program build, thus ensuring personnel levels adequate to cover the workload; b) review billet and position descriptions to ensure they accurately reflect the duties of incumbents; and c) participate in the planning and implementation of reorganizations. Supervisors also manage activities that affect the productivity of the workforce.

Management of space and equipment. Supervisor accountability for the condition of assigned work spaces and equipment often brings resource implications. Examples include funding for maintaining space and equipment, buying replacement equipment, and renovating workspace.

Contracting. Supervisors play a key role in arranging for contracts for the purchase of goods and services. They provide much of the information used to prepare the statement-of-work or statement-of-objectives that will accompany the request-for-proposal to be issued to vendors interested in bidding on contracts. A good deal of this information can be extracted from the project description in the original funding proposal.

Implementation of Spend Plans. Most supervisors use a "spend plan" as a management tool to maintain a running balance of available budget authority as the fiscal year progresses. This tool helps ensure the availability of funds at any given time to meet anticipated and unanticipated needs during the year. It alerts managers to potential shortfalls that may require additional funding or curtailment of some planned activities. Supervisors can measure how efficiently and effectively their subordinates manage their budgets by tracking commitment, obligation, and expenditure rates reflected in the subordinates' own spend plans.

Tying Everything Together

The author's work experience certifies the value of combining comprehensive with programmatic thinking to give life to the foregoing budgetary principles. Every intelligence supervisor and office director needs to develop a working familiarity with his or her home country's apparatus and processes for resource management. These same officials also need to develop an appropriate style of negotiating the unavoidable bureaucratic politics that accompany the competition for adequate funding of intelligence programs. They need to know how to engage counterparts who control the allocation of personnel and space (facilities), the use of occasionally contracted services, and other resources that can impact their ability to accomplish assigned missions and responsibilities. Finally, to meet effectiveness as well as efficiencicy goals, supervisors and office directors always need to relate resource management plans and decisions to the substantive side of the intelligence enterprise.

Epilogue

Effective funding proposals and the use of specific criteria for measuring a proposal's effectiveness can help both the preparing offices and reviewing officials. Efficiency and effectiveness of resource use needs the full attention of everyone in the chain of resource management because the ultimate source of funding and the reason for the existence of a national security and intelligence system are one and the same—our fellow citizens.

Author's Biography

Dan Elkins, a retired U.S. naval intelligence officer and nationally recognized expert on intelligence resource management, has experience in cryptology, imagery intelligence, resource and manpower planning, reserve management and coordination, and intelligence training and education. He has offered resource management courses at the Defense Intelligence College and its successor institutions (now the National Intelligence University) and the Joint Military Intelligence Training Center (now the Academy of Defense Intelligence) in Washington, DC. In February 1995, he founded DWE Enterprises, a consulting firm for the management of intelligence resources, and subsequently served as a faculty member of The Intelligence and Security Academy. Mr. Elkins has trained well over 10,000 U.S. Intelligence Community and Defense Department personnel, including congressional staffers, personnel from two national laboratories, and employees of a number of corporations. Mr. Elkins holds a B.A. in Spanish (1975) and an M.B.A. in finance (1980) from what is now the University of Massachusetts at Lowell. He is the author of the 2004, 2006, 2010 and 2014 editions of *Managing Intelligence Resources* (DWE Press), the nation's most authoritative consolidated reference on intelligence and defense resource management for the intelligence and defense communities. **Email:** *dwelkins2@cs.com.*

Changing Paradigms in Military Intelligence—Civil Affairs Operations and the Threat of Militarily Capable Criminal Groups

G.M. Capo

and

M.A. Duarte

"The supreme art of war is to subdue the enemy without fighting."

—Sun Tzu, *The Art of War*

Introduction

In Latin American countries, the absence of a state presence in underdeveloped, remote areas, coupled with the growth of corruption and infiltration by criminal groups, poses a continuing problem. Diminished capabilities of the armed forces and other public security institutions allow organized crime and drug cartels to flourish. Remote areas without a national institutional presence tend to fall under the control of nonstate actors who often develop power structures parallel to those of the state.[418]

The level of sophistication, technical competence, and overall capability of criminal groups in the region compels governments to consider them military entities by type and capability. With their equipment and tactical proficiency, their mobility and transborder reach, they constitute a totally operational army. The poor economic and fiscal capability of some countries in the region to finance their armed forces, and vestigial prohibitions and embargoes on military aid, obligate Latin American countries and their military establishments to find new means with which to confront well-financed criminal groups.

This scenario should be viewed as an opportunity for paradigmatic change. It provides an opportunity to rethink the use of military forces in national counternarcotics strategy. In place of a focus on the use of arms and its associated advanced technology, the military can apply intelligence to social problems in a way that permits the army to protect populations at risk. The military

can develop intelligence in geographical areas of interest to narcotraffickers by gaining a nuanced understanding and analysis of the residents' sociocultural, psychological, and economic needs and desires. In this way, armies of the region could establish themselves as the chief government representatives in remote areas at risk. They would gain the information and knowledge needed to bring aid and development to these communities. "Social intelligence" would thus give the armed forces an enduring capability to deny or at least hinder criminal groups from insinuating themselves into remote communities.[419] Could this paradigm usher in an effective strategy to break the economic power of transnational criminal networks?[420]

Background

The 1995 Framework Treaty on Democratic Security in Central America and the 1996 Guatemala Peace Accords initiated the country's pathway to democracy and its institutional transformation. It also instilled a new concept of security in the Central American region, centered on the protection and well-being of individuals.

A 1996 Agreement on Strengthening Civilian Power and the Role of the Army in a Democratic Society[421] demilitarized Guatemalan society and brought on a new National Security System (SNS). However, 12 years had passed before the Framework Law for the National Security System (Decree 18-2008) finally allowed the state to confront security challenges through coordinated actions at the highest levels of government.[422]

The Framework Law established the SNS and a National Intelligence System (SNI). Both operate under a democratic security paradigm primarily focused on the protection of individuals.[423] Together, the treaty, peace accords, and framework law offer theoretical support and legal authorization for government action and provide a pathway for social intelligence.

More recently, the Guatemalan National Security Council outlined a strategy for how the country can prevent and counter various risks and challenges to the state in a National Security Policy document.[424] The Advisory and Planning Commission (CAP)[425] then presented a strategic security agenda and plan to complement the principles and strategic objectives outlined in that document. Together, these documents embody Guatemala's security strategy.

By extending the model of democratic security in its preventive form, orienting the state's actions, and establishing the fundamentals for a continual evaluation of efficiency and effectiveness through planning, these recent documents are historically transcendent. The National Security Policy has established a strategic direction for intelligence. Social intelligence implements one aspect of that strategy.[426]

Consequences for the Armed Forces

Given the lack of an explicit separation between military and police spheres of operation, the Guatemalan Army can at any time take action to preserve internal security. The armed forces for an extended period have not been used to defend the state or its citizens against external foes. A 2012 Protocol for Inter-Institutional Engagement (Accord 285-2012) addresses army support to civilian security forces and updates the authority of the army as an actor in internal security.[427]

The prestige and capability of the armed forces suffered from an Army Modernization and Transformation Plan (No. 3-"H"-01) of 2004. The plan imposed a drastic personnel reduction, but the projected "modernization" never took place. The Guatemalan Army shrank from 27,000 soldiers to 15,500. The transformation plan considered the new number reasonable in view of the personnel complement of other armed forces in the region. The plan negatively impacted not only the military institution but national security itself. The state lost its ability to maintain a dissuasive presence throughout the national territory.

Meanwhile, the Peace Accords and Agreement of 1996 had set the course for the creation of the National Civilian Police (PNC). The PNC replaced the National Police, an organization that had failed to address societal needs under a democratic regime. Decree 11-97 established the PNC and charged it to "protect the life, physical integrity, and security of persons and their property, ensure their free exercise of rights and freedoms, and prevent, investigate, and fight crime, thereby preserving public order and public security."[428] From the start, this police force has experienced serious deficiencies. In particular, it has not established a permanent presence throughout Guatemalan territory, thereby facilitating the incursion and implantation of criminal elements and organized crime groups in several parts of the country.

The PNC has three responsibilities: prevention of crimes, investigation of crimes, and maintenance of public order. Although it has been addressing its deficiencies by developing reform initiatives, the society at large has not recognized this progress.[429] The weaknesses of the PNC result from organizational deterioration and lack of coordination during the transition period from one government to the next. A study measuring the confidence of citizens in societal institutions on a scale of 0 to 100 found that political parties in Guatemala earned a rating of 36.1, congress a 41.9, and the PNC only a 34.9. In contrast, churches (Evangelical and Catholic) received the highest ratings at 64.0 and 70.2, respectively, while the army nearly equaled those with 59.5 points.[430]

Police weaknesses place the force in a vulnerable position as citizens question its legitimacy and credibility. A special Presidential Commission formed to correct the problems faulted weak professional development of the force as the chief reason for the inadequacy of police reform.[431] A notable deficiency appears in teaching and learning the requirements of a criminal justice system. Inadequate development of criminal investigation capability begins with police training but extends to the entire National Civilian Police operation.[432]

Any comparison of army capabilities with those of the PNC would find that only the national military organization possesses the human and material resources needed to ensure citizen security in the face of militarily capable organized crime and drug-trafficking groups. Only the army can prevent the incursion of criminal elements and allow for long-term socioeconomic development of rural populations. The army lacks only a strategy for collecting preventive social intelligence information and knowledge within a democratic, rule-of-law model.

Civil Affairs in Guatemala—Unique in Latin America

A Guatemalan civil affairs doctrine first apeared in 1955, when a Governing Accord (Army General Order No. 17-17) created the Army Public Relations Department within the Ministry of National Defense. During the 1960s and 1970s, Guatemalan civic action projects followed models based on U.S. Army doctrine. In 1971, the first Civil Affairs Operations Manual advocated developing a closer relationship with and obtaining greater support from the public.[433]

Civil affairs focused on the country's internal situation, but reflected the international Cold War environment. The United States, seeing a rapid advance of communism in places relatively near U.S. territory, put in place a grand strategy to contain the advance of this ideology. The strategy —known as the "National Security Doctrine"—was imposed on and accepted by Latin American armies, giving them an identity and the sense that military institutions were responsible for the destiny of their respective nations.

In the 1950s, the first national intelligence services of the modern era also appeared in the region. They focused on the internal environment in each country. In the 1960s, under the influence of the National Security Doctrine, the region's intelligence systems grew in personnel, technology, specialization, and budgets. The idea behind the Pentagon's strategy, that the "internal enemy" had penetrated all spheres of society, led the intelligence services to strengthen themselves further and to extend their reach into new areas. Cold War-era "social intelligence" began to operate in political, economic, and social spheres, as well as in the military realm.[434]

Civil affairs units in Guatemala operated under doctrinal principles originating in Taiwan, whereby the so-called "political war" saw the winning of territory as less important than winning the minds of the people.[435] That is, strategic advantage comes not from success on the field of battle but from understanding the fabric of society. Prosecuting a political war does not imply a non-violent approach. Rather, any violence should remain limited. The avoidance of direct military confrontation would hopefully advance the desired political outcome.

The 1980s became the most critical decade for the internal Guatemalan conflict. Ideologically focused campaigns became "psychological operations." The Office of Civil Affairs emerged within the General Staff of National Defense (D-5) and appointed the first civil affairs officers. These officers conducted psychological and propaganda operations. In conjunction with these operations, "social intelligence" appeared as a means to understand social conditions that might create friction among population groups, and to guide the use of preventive measures. In 1983, the first 11 Civil Affairs and Local Development Units operated in the principal military zones of the country.[436]

In retrospect, social intelligence epitomized the army's changed approach to tactical situations, where minimum force was to be used against localized resistance. An analysis based on the information provided by the Civil Affairs Units about each village, town, and city guided the unit's response to inhabitants' needs. Social intelligence collectors explored each population center to acquire knowledge and an understanding of conditions and causes that favored the growth of conflict; that is, social intelligence detected potential discontent. These preventive units linked all the information they acquired in their areas of interest to the army's intelligence system. All the resources of the Civil Affairs Units were, in effect, oriented toward social intelligence.

Civil Affairs Units in the Guatemalan Army had more fully trained and experienced specialists than any other country of Latin America. The Guatemalan Army served as the permanent site for the Subcommittee on Civil Affairs associated with the Annual Conference of the American Armies. However, in the force restructuring of 2004, these units were demobilized. In their place, the School of Public Relations began to operate under the Regional Peacekeeping and Peace Operations Training Command. The school prepares Guatemalan Army and selected foreign officials for work in civil affairs and psychological operations. Its graduates focus on civic improvement projects, local development, and giving advice to community groups and working committees, as well as maintaining institutional ties to the population.[437]

Although the School of Public Relations and the Office of Civil and Military Relations of the General Staff of National Defense, together with the Manual for Civil Affairs (ME-20-02, authorized in 2011), have modified the doctrine for new army missions and scenarios, civil affairs lacks the personnel, materiel, and leading technologies of past decades. The main explanation lies in the reduction of army personnel, which affected civil affairs capabilities. The decision to reduce the military apparatus also undermined adequate geographic coverage of the country by military units. During the years of internal conflict, military units deployed throughout the country, and especially in zones of conflict. Six of the fourteen military zones were deactivated in the 2004 retrenchment.

The government now innovates by creating specialized brigades and interinstitutional task forces. Of two brigades created in 2012, one focused on environmentally "protected areas" like the *Laguna del Tigre* in the Petén and on

the eradication of clandestine runways used by narcotraffickers. A new military police brigade began work in the *municipios* of Guatemala City. Starting in June 2013, two more new brigades deployed to address border security. A brigade of marines monitored the beaches and inlets of Atlantic and Pacific coasts. An Army High-Mountain Brigade began extensive patrols to control and eradicate the planting and harvesting of opium poppies and to reduce field laboratory production of illegal synthetic drugs. An interinstitutional task force initiated work with the National Civil Police, the attorney general, and the Tax Administration. It aims to reduce contraband commerce, narcotrafficking, and arms trafficking along the border with Mexico.

These actions are having limited impact. Criminal groups have greater resources in technical and materiel terms than state security organizations. The preventive Community Relations Intervention Division[438] of the National Civilian Police cannot yet deploy widely enough to address security problems in remote areas. In October 2012, when security forces tried to resolve a social protest in the Department of Totonicapán area known as the *Cumbre de Alaska*, six deaths occurred. The operation brought to light a lack of coordination combined with a lack of information and intelligence.[439] Across the larger region, countries do not have a financially sustainable capability to continue a direct-action, frontal battle of attrition against drug trafficking and related transnational organized criminal groups.[440] Armies have very limited resources or do not receive useful levels of international technical and materiel support.

A "proof of concept" demonstration of the utility of social intelligence could alert citizens to the value of preventive information in augmenting the state's scarce security resources. Gaining the reciprocal assistance of local populations would further assist the state's capability against internal and transnational threats.

An Altered Paradigm—Civil Affairs-Based Strategy for Prevention and Defense

Militarized drug cartels have vast capital resources, illicit arsenals, command and control equipment, and armored vehicles for tactical mobility. They have become war-fighting entities with solid military capabilities.[441] This reality demands a renewal of armed forces and other security institutions'

capabilities. Any new or altered strategy should facilitate an efficient and respectful relationship among the armed forces, government, and citizenry.

To address the criminal threats that endanger the country's inhabitants and threaten the stability of governmental institutions, the authors have proposed a program of civil affairs-led military operations. The operations will have the flexibility and power to carry out preventive, intelligence-based actions. The program coincides with the country's strategic objectives. Similar programs exist in Colombia and Peru, where Civil Affairs Units (generally with U.S. support to local military units) have played an important role in the fight against cartels and transnational organized crime groups. However, those programs only respond reactively to criminal groups who seek competitive advantage over the state in addressing the vulnerabilities of local populations.[442]

In contrast, the authors' proposal for Guatemala, and possibly for neighboring countries, establishes a program that takes advantage of the multidisciplinary capabilities of the state. It uses the institutional structure of the armed forces and remains within the existing legal framework. The recommended approach supports a positive, preventive relationship between the armed forces and civilian authorities, and with the population in general. The authors expect that planning, support, and implementation of activities, operations and projects will promote the development of disadvantaged populations, thereby reducing criminal exploitation of their vulnerabilities.

Inter-institutional task forces, where police and military officials cooperate and share responsibilities, have a limited purpose suitable to particular times and places. Civil affairs units operate as a part of a larger institution, have a defined mission centered on prevention, and generally have a permanent structure. Military personnel of civil affairs units are soldiers first, and their mission is to support their commander and certain civilian institutions, although they are not part of the latter. The principal task of civil affairs personnel is to obtain information about a local social environment to verify intelligence reports or to contribute to military intelligence or the national intelligence system at large. Civil affairs units operate exclusively within the armed forces. When civil affairs personnel no longer support a military commander, any civilian organization that might need their services can employ them, but as civilians.[443]

The authors propose the programmatic use of military civil affairs operations, led by intelligence teams, to focus on understanding the social environment at risk. Civil affairs teams can engage local populations in a collaborative effort to avoid or deny the penetration of communities by narcotraffickers. Simultaneously, the teams can manage and improve the image of the army and the central government. The intelligence-based, civil-affairs approach identifies local problems, prioritizes them, and finds solutions. The best solutions will come from suggestions offered by those who live in the places at risk. Social intelligence builds and depends on reciprocal collaboration with everyday individuals and officials in diverse localities.

In Guatemalan defense ministry terms, any entity supported by sufficient resources, organization, and intentions to challenge the state's attainment of its fundamental objectives constitutes a *threat*. Narcotrafficking and organized crime, in that order, pose the most serious challenge to Guatemalan security. The minister of defense believes that neither has yet risen to the level of a threat because neither has the capability to oppose conceptually or ideologically the national objectives of Guatemala.[444]

Not all Guatemalan communities susceptible to criminal influence are actually targeted by the narcotraffickers. Instead, they target only those communities in locations of strategic criminal interest. Narcotraffickers give financial support to projects that benefit citizens in those areas. They often cooperate with local Municipal Development Councils (COMUDES) or Community Development Councils (COCODES).[445] Narcotraffickers gain social status by building hospitals, roads, and bridges quickly without bureaucratic impediments. Although they may not yet have become a threat, narcotrafficking and organized crime remain among the chief concerns of political figures in the country.

For the Guatemalan army, and for countries with a similar social environment, civil affairs units can be a "secret" weapon and a source of power. The *modus operandi* of social intelligence enables information collection without reference to an "intelligence operation." Its mission is to observe, analyze and communicate social details related to the prevention of crimes and violence—nothing more and nothing less. The centerpoint of civil affairs strategy is the concept of "minimal force."[446] The civil affairs hosting of a social intelligence

capability signals the army's intention to support local actions and institutions on a continuing basis. Although civil affairs operations do not totally renounce the use of force, they can best act as "shock absorbers" for the local population when confrontations or conflicts occur.

The army is well suited for implementing a social intelligence program for two reasons. First, this institution typically has a real and reinforceable presence throughout the country. Second, it typically possesses a more robust organizational capability than other state institutions.

Some individuals or groups in Guatemala may remain unprepared for the authors' proposal, or will simply not find it acceptable. They may see it as a shift toward greater militarization or re-militarization of the National Security System. Discussion of Guatemalan military policies always elicits strong and antagonistic opinion. The shadow of internal armed conflict of decades past has not yet faded. Additionally, the generally conservative, slow-to-change armed forces hesitate to accept new cognitive or behavioral paradigms. Nonetheless, the authors know that the armed forces identify with the democratic values and beliefs of the society of which they are part. Many citizens understand military values and even identify with them. Yet the military as a professional organization stands apart from making hasty or vengeful judgments and can readily refrain from damaging involvement in local politics. The authors' proposal expects the armed forces to serve the national political purpose of democratic security through respect for the rule of law and human rights and a focus on the protection of the individual.

In 2012 the High Command of the Army received and accepted the authors' proposal.[447] Preparation of personnel to implement the program soon followed. Even though a similar program existed in relatively recent Guatemalan history, the legal basis, operating principles, doctrine and purposes of the new program differ substantially. Authoritarian or arbitrary methods were applied in Guatemala by earlier civil affairs units, with little or no protection of human rights. Today, a state-centric vision has evolved to an ethno-centric approach that favors the protection of individuals and families.

Summary

The authors recommend social intelligence as an alternative to the traditional military intelligence approach to internal security in Guatemala. Only the

armed forces have the capability to confront criminal groups that themselves have real military capabilities. Civil affairs units of the army offer an appropriate home for social intelligence activity. Civil affairs units can be effective in undertaking public security activity because the military enjoys a better public perception than any other public security force in Guatemala. Also, only the military can deploy anywhere in the country for an extended period and perform in strict compliance with a national doctrine, under a constitution and with supervision by elected civilian authorities.

This proposal does not seek to expand the influence of the armed forces at the cost of restricting the authorities of the National Civil Police. Instead, it seeks to reactivate and strengthen a capability of the Guatemalan military structure that was dismantled in 2004. The army's civil affairs units cannot usurp the functions of civilian security forces. To do otherwise would expand the mission of the army to areas of responsibility that remain exclusively civilian.

The authors also do not suggest the use of force by the civil affairs units although they have the right to its use. Instead, civil affairs development of social intelligence will simultaneously promote the aims of national development and the aspirations of rural communities across the country. Finally, the ability of this proposal to renew the prominence of civil affairs depends on strengthening the superstructure of the army and the National Security System.

Epilogue

Editor's note: Following the acceptance of this essay, the authors submitted an addendum to their work, in which they describe an implementation model for social intelligence in Guatemala.

System for Humano-Social Understanding (SES-H)

The SES-H model offers a multidisciplinary management, analysis and evaluation tool for the holistic understanding of designated regions in Guatemala. It will benefit development projects and help maintain peace in rural and urban areas. Implementaton of the model does not depend exclusively on the armed forces, although institutional support from the army may help in some situations. The model aims to reinforce inter-institutional coordination so that state and local authorities and private industry will make long-term

investments in local communities. The model aims to strengthen citizen participation and guarantee long-term human development in targeted regions.

The model recognizes that the army's civil affairs units exist to anticipate and find solutions to security problems within the country. The authors also recognize that successive governments have found it difficult to carry out sustainable and long-lasting programs for community development in the regions where a state presence has declined or been lost. When government institutions are absent, the resulting lack of authority and control negatively impacts the life and property of individuals, democratic institutions, the rule of law, and human rights.[448] In addition, the lack of problem-solving government services and programs means that the affected communities seek other, informal or illegal ways to obtain services. This process creates a culture of illegality among citizens. A culture of illegality corrupts community life and brings violence, abuse, and the denial of services as a means of enforcing informal authority. The SES-H program can anticipate the emergence of conflicts associated with this syndrome.

Basic Aspects of the Model

Functional areas

The SES-H model integrates information about a specific geographic area from six functional areas. The synthesized information allows a team to achieve deep understanding of the social, cultural, economic, and historic complexities of an area and its population. The six functional areas are:

- Geographic space
- Local background and history
- Social interactions
- Local culture
- Political forces
- Economic dynamics.

Management

- *Board of Directors*

Provides for coordination, control, and general management of the SES-H team

- *Analysis*

Component for fusion, analysis, and dissemination of information

- *Collection*

This approach depends on a deployed field component, made up of teams responsible for collecting information in the designated geographical area. Each team includes a chief and six specialists, one for each functional area.

Personnel

Because the SES-H model emphasizes management and analysis, personnel at all levels require experience and professional development suitable for the respective functional areas. Military or governmental experience can be beneficial in some instances. Members of the Board of Directors require certification in management, analysis, and collection. Personnel working in analysis need a strong work ethic, a concern for detail and familiarity with all available tools for analysis. Finally, field information collectors need experience in each of the six functional areas of concern to the holistic effort. In addition, given the supreme difficulty in finding capable individuals who know each local area in detail, the team should seek out a trusted local adviser for each deployment.

Application

The authors monitored the activity of an SES-H team fielded to a holistic development area in rural Guatemala, and advised the military commander responsible for the corresponding security task force located in the capital city. They expect the establishment of a more autonomous SES-H team in the rural northeast.

Biographies of the Authors

M. A. Duarte, a doctoral candidate in strategic security at the *Universidad de San Carlos de Guatemala*, holds an MBA from Rice University with a focus on strategy. He also earned a BS in industrial engineering from the University of Houston. He has worked on national security projects with the U.S. Department of Homeland Security and the U.S. Department of Defense. He authored *AHORA: Evitando los riesgos de una sociedad insegura* (Grupo Litopogra, 2009) and now heads the Office of Monitoring and Communication at the Technical Secretariat of the Guatemalan National Security Council. **Email:** *andresdugar@gmail.com.*

Grisel M. Capo, a doctoral candidate in strategic security at the *Universidad de San Carlos de Guatemala*, earned a master's degree in international relations with a focus on international cooperation from the *Universidad Rafael Landívar de Guatemala* and a bachelor's in international relations from the *Universidad de la República Oriental del Uruguay*. She is a graduate of the Center for Hemispheric Defense Studies (Perry Center) in Washington, DC and has studied civil-military operations at Fort Benning, Georgia. She has authored several articles on intelligence themes. Presently, she serves as a consultant on external security to the Advisory and Planning Commission of the Guatemalan National Security Council. **Email:** *griselcapo@hotmail.com.*

Intelligence Cooperation in the Framework of the Union of South American Nations (UNASUR): Possibilities and Limitations

Carolina Sancho Hirane

"Axelrod, speaking about cooperation, begins with a key question: "Under what conditions will cooperation appear in a world of egoists, without a central authority?"[449]

"European countries are increasingly accepting that risks and threats today are not different for each country, but they are transnational, and that shared risks can only be addressed by a common approach."[450]

To explore the possibilities and limitations of intelligence cooperation within UNASUR[451] this study will identify the elements required for its effective development. One compound question will guide this examination: "What are the obstacles to effective intelligence cooperation in UNASUR, and how may they be overcome?" The answer to this question will represent the minimum requirements for cooperation to be effective.

Intelligence cooperation does take place among many countries that make up UNASUR, but considerable room exists for qualitative and quantitative improvement of cooperation within its framework. Intelligence cooperation occurs under formal or informal circumstances as member countries seek the capability to prevent consensually defined dangers to their security. At this time, no formal mechanism for intelligence cooperation exists in UNASUR.

The essay begins with an exploration of intelligence cooperation theory. A review of the relevant academic literature, to include typologies ascribed to the phenomenon, will develop an understanding of its basic elements and their applicability to the question of managing intelligence cooperation in UNASUR.[452]

Theoretical Aspects of Intelligence Cooperation

National intelligence agencies and programs engage in both cooperation and competition with those of other countries.[453] States resist intelligence cooperation because they prefer not to subject their own intelligence agencies to foreign requirements. They also resist because they face the already difficult question of how much information each country should collect on its own population and how much should be exchanged among its own executive agencies. In this environment, having to decide how much information should be exchanged with foreign agencies may appear too daunting. Nonetheless, interagency relationships and exchanges do occur as a normal part of bureaucratic process in any country, and every country learns to handle the question of how individual intelligence services can best process and disseminate information they obtain.[454]

New threats pose challenges to security agencies, and in order to improve their efficiency they may need to share information and/or operations with foreign services. To create, deepen and improve these international ties is one of the chief ways to meet the threat posed by terrorism, organized crime, and narcotrafficking. Those ties require thoroughgoing cooperation to be effective, but a capability to manage the information flow and coordination required to address mutual threats requires time to develop and must accommodate the different ways agencies interact with one another.

Intelligence cooperation within the framework of multilateral organizations is not a new phenomenon. For example, the idea of a United Nations intelligence service emerged in North America near the end of the Cold War.[455] But because of internal tensions that the proposal generated within the UN, it did not gain traction.

Thus, the idea of intelligence cooperation in multilateral organizations is a recurring theme in how public safety worldwide might be ensured against transnational threats.[456] Academic publications frequently address the issue. Some countries have an urgent need to engage in intelligence cooperation to reduce their vulnerabilities and take advantage of opportunities, especially with respect to international terrorism. Reinforcing the value of intelligence cooperation against transnational threats such as terrorism, one author advises that

> the U.S. Intelligence Community, together with other intelligence services, need to work on creating a database that identifies and tracks foreign combatants, their known associates and spiritual mentors. If this database had been created during the Cold War, the United States would have been much better prepared for the subsequent terrorism campaign of al-Qaida.[457]

The former director of the UN Weapons of Mass Destruction Commission in Iraq, Hans Blix, has experience with intelligence cooperation. His commission interacted with national intelligence services to provide background information and data that contributed to national reports on subjects of multilateral interest. He found that the commission could not rely exclusively on information or intelligence from individual countries because they have interests different from those of the multilateral organization. However, his UN organization did not and does not have sufficient information tools to meet its objectives and has no alternative but to accept information from individual countries, and on that basis, take a stand.[458]

As he reflected on the best structure for effective information cooperation within multilateral organizations, Blix determined that the formation of a multilateral intelligence service with agents or officials from national intelligence services would lead to its having little international credibility. This is because, from the point of view of the international community, national intelligence services are simply acting *through* rather than *for* the multilateral organization, negatively affecting its professional image. This issue remains even when positive steps have been taken to improve multilateral intelligence capabilities.[459]

The participation by national intelligence service officials in a multilateral organization can be a first step toward building an atmosphere of cooperation in the organization's early stages. Intelligence officials with ties and allegiance to the multilateral organization itself can initiate a second step in that direction as they advise the organization's leaders on issues of strategic interest. The experience of the United Nations in peace operations demonstrates the limited utility of the intelligence function within that multilateral organization, which still does not field its own cadre of intelligence specialists.[460]

UNASUR could extrapolate some examples of intelligence cooperation from other multilateral organizations, but has not yet done so.[461] The Argentine observer Ugarte does point out, however, that one of the specific objectives of UNASUR's South American Defense Council (CDS) is "to promote the exchange of information and analyses about the regional and international [security] situation, for the purpose of identifying the factors that can affect regional or world peace."[462] Ugarte further notes that the CDS's Center for Strategic Defense Studies (CEED) recognizes the relevance of strategic analysis and strategic intelligence for several of its areas of responsibility.[463]

Intelligence cooperation under the auspices of UNASUR is therefore feasible, pending a careful review of its possibilities, limitations, and the manner in which it may be carried out. A necessary condition will be for its benefits to outweigh any drawbacks for the actors involved. Pulido makes the interesting point that "if the relative gains obtained by each state from the process of intelligence cooperation do not in the long run produce a clearly evident improvement in the relative position of some countries over others, or even the perception of such an advantage, then the cooperation may be effective."[464]

The academic study of intelligence as a theoretic and applied discipline may contribute to multilateral cooperation in the region.[465] Academic study can advance the analysis of threats, vulnerabilities, and opportunities on behalf of the countries that make up UNASUR. Discussion and understanding of these aspects of South American security can become the basis for thoughtful management of common, multinational actions.

Typologies of Intelligence Cooperation

Intelligence cooperation, understood as the "willingness and ability of diverse organizations and intelligence professionals to work together to achieve common objectives,"[466] "is never without limits, no matter how strong the alliance between countries, or among the set of countries engaged in cooperation."[467] With these basic ideas in mind, cooperation may be categorized across three dimensions:[468]

A. Degree of formality of interaction, across a continuum from formal to informal. Informality corresponds with the absence of accords, agreements, or acts that would identify explicit institutional interests

in exchanging information between intelligence services. In practice, formal arrangements for cooperation are often discounted in favor of more flexible ways to engage, regardless of existing, formal treaties. Similarly, formal, permanent and very close cooperation, clearly a rarity, requires a strong commonality of interests and foreign policies between or among participating countries. An example of formal cooperation occurs when the agents or representatives of one service temporarily join another country's intelligence service.

B. Number of actors involved; that is, either a bilateral or multilateral relationship. Not surprisingly, on a worldwide basis, intelligence cooperation is mostly bilateral. Multilateral cooperation, considerably rarer, presupposes a strong alliance and generally strong ties among the participating countries.

C. Substantive activities in which partners engage. Three spheres of activity dominate intelligence action, each defined by respective targets of interest. These spheres correspond with the three great needs that are addressed by any country's intelligence services: military intelligence, strategic intelligence, and police or criminal information.[469] The table below does not acknowledge overlap among the spheres. Naturally, a more nuanced depiction would allow for less clear-cut distinctions. For example, in Mexico, the armed forces and by extension, military intelligence, both have interest in narcotrafficking, a criminal activity that is usually the responsibility of the police. A similar situation may be found in Colombia.

Table 11
Characteristics Differentiating Military, Police and Strategic Intelligence Services

	Military Intelligence	Police Information	Strategic Intelligence
Chief target	Threats	Crimes	Threats and crimes
Asset protected	Borders	Public order	State security
Threat origin	Exterior	Interior	Interior - exterior

Table 11
Characteristics Differentiating Military, Police and Strategic Intelligence Services (continued)

	Military Intelligence	Police Information	Strategic Intelligence
Product provided	Instrumental	Instrumental	Final
Purpose of its action	Preventive-reactive	Preventive-reactive	Preventive
Judicial mechanisms	No	Yes	Sometimes

Source: Antonio Diaz, Miguel Revenga, Oscar Jaime, and Rafael Martinez, "Hacia una política europea de inteligencia," *Revista Política Exterior* (Spain) XIX, no. 106 (August 2005).

Diaz additionally identifies three levels at which multilateral intelligence cooperation may occur:

1. Through cooperation at the *macro* level, based on international agreements or treaties. This level implies that multilateral agreements have the purpose of establishing a framework for the exchange of information or even other forms of cooperation that may take place between intelligence services;

2. Cooperation in operational practices and processes takes place at the *meso* level. Cooperation at this level involves the standardization of methods of communication and creation of reports, the timing and periodicity of meetings, and the regulation of permanent contact with liaison officials;

3. Cooperation at the *micro* level refers to the conduct of individual investigations or actions such as provision of information with respect to specific cases. As an illustration, "Decisions will often be made on an ad hoc basis at relatively low organizational levels to resolve concrete situations as they arise."[470]

To summarize, typologies of intelligence cooperation can be viewed from different perspectives, according to the level of formality at which it is

institutionalized, the number of actors (countries) that participate, the spheres or subject matter areas in which it takes place, and the bureaucratic levels at which it takes place. Taken together, the various perspectives allow us to identify the density of intelligence cooperation in different geographic areas covered by any agreements.

Limitations and Possibilities for Intelligence Cooperation

South American intelligence cooperation in multilateral organizations has historical roots in the East-West conflict.[471] Intelligence cooperation between South American countries and the United States rested on ideology, that is, to prevent communism from being a viable political option in the region. The region has not seen major changes in the realm of intelligence cooperation since that era, despite the emergence of the Community of Andean Nations (CAN), the Common Market of the South (MERCOSUR), and expanded MERCOSUR.[472]

U.S. hegemony continues through various initiatives to share information and intelligence, whether through offices or organizations headed by the United States, or through the Organization of American States.[473] The opportunity to improve the level of mutual confidence grows as South American intelligence officials get to know one another more directly than usual under the auspices of organizations such as the Inter-American Drug Abuse Control Commission (CICAD), the Joint Inter-Agency Task Force-South (JIATF-S), or the Inter-American Committee against Terrorism (CICTE). In the same way, the basis for intelligence cooperation between and among South American services may grow in other venues where intelligence specialists and their supervisors get to know one another.

The European Union (EU) offers positive experiences in intelligence cooperation through multilateral organizations that address common threats. For example, the European Police Office (EUROPOL) and the European Situation Center, among others, show the feasibility of multilateral cooperation in intelligence. The next section examines the EU experience in intelligence cooperation. That experience illustrates the range of possibilities for cooperation once the minimum requirements for its success are met. Those requirements include a convergence of security, defense and foreign relations policies, along

with some homogeneity in the security practices of intelligence agencies and the professional capability of their officials.

The European Union and Intelligence Cooperation

European arrangements for intelligence cooperation originated primarily as a way to avoid situations that might lead to devastating armed conflict among the Europeans themselves. These arrangements began with the multilateral control of the main elements of the arms industry, steel, and coal (European Coal and Steel Community), in the early 1950s. In 1993 Europe achieved a transcendental milestone when the European Union (Maastricht) Treaty went into effect. Today, the EU counts twenty-eight countries from across the whole continent as members.

The EU's construction of an intelligence capability, through committees, working groups and monitoring installations, has been a long-running enterprise, both gradual and meticulous. Another aspect of the EU's approach to cooperation has played a vital role in its activities: Each cooperative act, exchange of information, and any participation in the EU's various communitarian organizations occurs on a totally voluntary basis. In other words, no member state feels obligated to agree with or participate in any type of EU initiative.

The U.K. Parliament, and the EU itself, have established guiding principles to achieve successful cooperation in intelligence. The British identify four principles: 1) confidence in human-source intelligence; 2) awareness that intelligence and politics are intrinsically linked; 3) agreement that intelligence ethics are important; and 4) a need for joint intelligence capabilities to be accessible to all cooperating partners. The EU has developed five principles to guide intelligence cooperation: 1) solidarity among the states of the EU; 2) voluntary contributions by each state; 3) clear understanding of the terrorist threat and full use of available threat analyses; 4) coordination among the institutions that have the common objective of combating terrorism and collaboration with appropriate partners; and 5) respect for the appropriateness and effectiveness of the other four principles.[474]

The cooperative process of identifying threats faced by the continent has become a central theme in European political, social, and cultural discourse.

The process strengthens the EU's fundamental political will to cooperate. Multilateral cooperation also responds to the idea that today's transnational threats are not geographically circumscribed; that is, they are global. They range from Islamist terrorism, illegal migration, cybercrime, and organized crime to climate change, piracy, food shortages, resource security, disease, and pandemics.

Confronting these threats contributes to the economic security of the continent. Regional economic instability can endanger "European interests," as pointed out by William Shapcott, former director of the EU Situation Center (SitCen), a strategic analysis organization.[475] The EU has adopted a continuous intelligence-based review and analysis of several themes: 1) military security; 2) economic security; 3) internal security (terrorism, chiefly radicalism or extremism); 4) technological security; 5) operational security during peace talks and during periods of military tension; 6) counterespionage; and 7) information security.[476]

Impetus for Strategic Intelligence Cooperation

An early push for EU interstate intelligence cooperation came from the Club of Berne, created in 1971. This club each year brings together the intelligence service directors of all EU member countries to establish an agenda for continental security cooperation. In 1999, it began to address terrorism, interception of communications, encryption, and cyberterrorism. Since 2000, additional questions related to the role of intelligence agencies in European integration have been added to the agenda.[477]

European Union Intelligence Analysis Center (EU IntCen)

The Situation Center became the EU's first permanent organization designed for strategic intelligence analysis. It was created in the 1990s under the banner of the Western European Union (WEU), a defense and security organization formed by the member states of the EU and the North Atlantic Treaty Organization. In the words of its founder, the Situation Center "produced intelligence analysis in support of European policies."[478] Its mission remains the same today, but its name has changed to the European Union Intelligence Analysis Center (EU IntCen).

Since 2011, the EU IntCen has been part of the European External Action Service (EEAS).[479] It provides intelligence analysis, early warning, and situational awareness to the High Representative of the EU, as well as to the EEAS itself and to various EU decisionmaking bodies.[480] The EU IntCen synthesizes civil and military intelligence in real time and it can go operational in crisis situations. Operationally, it safeguards the internal security structure of the EU, and strategically it helps ensure a supranational, European viewpoint by uniquely addressing the variety of threats that affect the EU. It accomplishes this objective by taking into account the threat data that the different national intelligence services of the states choose to make available to it.[481]

Some national intelligence services resisted sharing information with the Situation Center. That is why only some countries sent liaison officers to the center. Notably, the intelligence services of some member countries lack precisely the joint vision that permeates the central organizations of the EU. The SitCen did arouse suspicions at the political level in 2010 when the European Parliament ordered a study to learn how to improve the surpervision of its activities. Until that time, the SitCen had acted without any democratic controls.[482] However, with its conversion in 2011 to the EU IntCen, and its advising the High Representative of the EU, it gained prestige.

A European Intelligence Agency

The creation of a supranational EU intelligence agency is under discussion. The debate peaked with terrorist attacks like those in Madrid (2004) and London (2005). Even the European Parliament, when it launched an investigation into the alleged Echelon collection activities,[483] observed that "it is inconceivable that the intelligence services should be the last and only area not affected by the process of European integration."[484]

The idea of a European intelligence agency arose in the 1960s when a few NATO officials suggested the establishment of a more coordinated way to share intelligence in Europe. However, suspicions of the Cold War and rivalries between the United States and France quashed the idea.[485] After the fall of the Berlin Wall, the idea appeared again, but in an academic environment. The academic vision of an European agency expected it would "coordinate and analyze information submitted by other organizations and

foreign intelligence services, and only eventually would it be able to collect its own information.[486]

Smaller and less developed states, such as Austria, Belgium, Greece, and Ireland, have promoted the idea of a European intelligence agency.[487] Those countries have several times raised the possibility of such an agency. However, evidence now suggests that there will be no European intelligence agency because the larger countries, especially Germany, Spain, France, United Kingdom, and Italy, known in intelligence circles as the G5, place more trust in their own national intelligence capabilities and doubt the positive effect of a supranational organization. They feel that it would only duplicate national efforts and subsidize the intelligence agencies of the weaker countries. Other asymmetric factors add to the doubt. Only eight of the twenty-eight member states of the EU have a foreign intelligence service. Further, the main intelligence focus of Nordic countries but not of others is in the area of police intelligence. These uneven organizational and functional characteristics across the region increase the difficulty of intelligence sharing.[488]

Today the EU presents an interesting if not completely convincing model for cooperation in many spheres of intelligence. Although as a model, EU intelligence cooperation is still evolving, one can clearly see evidence of cooperative activity at the meso and macro levels, as defined by Diaz.[489] The EU operates with a relatively advanced level of intelligence cooperation as a result of its harmonization of security and defense policies, as well as the high-level coordination of those policies. Some of these practices may come to enlighten potential cooperative relationships in intelligence among the UNASUR countries.

A Basis for Intelligence Cooperation in UNASUR

Ugarte remarks that "no institutional mechanisms for intelligence cooperation have emerged in UNASUR, nor does any existing intelligence cooperation rest on the integrative impulse of this organization."[490] However, at least four motives argue for potential intelligence cooperation in the UNASUR framework.

The first motive comes from the existence of threats, risks, and vulnerabilities to the security of member countries, together with feasible opportunities for

intelligence cooperation suggested in UNASUR's foundational document. Its paragraph "q" calls for

> [c]oordination among the specialized organizations of the member states, in keeping with international norms to strengthen the fight against terrorism, corruption, the worldwide problem of drugs, human trafficking, trafficking in small and light arms, transnational organized crime and other threats, as well as disarmament, non-proliferation of nuclear weapons and weapons of mass destruction, and de-mining; experience among many South American countries in intelligence cooperation may be brought into play under UNASUR.[491]

Three other paragraphs in the same document indicate an interest in defense cooperation: s) "… the exchange of information and experience in defense matters," together with t) "cooperation to strengthen citizen (public) security," and u) "sectorial cooperation as a way to deepen South American integration through the exchange of information, experiences, and professional development."[492]

A second motivation for intelligence cooperation in UNASUR comes from the existing intelligence capability of each South American country. In general, most countries are already capable of intelligence cooperation in each of the three categories of military intelligence, police intelligence, and strategic intelligence.[493] The table below reveals which countries have well-developed intelligence systems.

Table 12
Members of the Intelligence Community or System in each UNASUR Country

Type of Intelligence Country	National Agency	Military Intelligence	Police Intelligence	Foreign Relations	Financial Intelligence
Argentina	X	X	X		
Bolivia		X	X		
Brazil	X	X	X	X	X

Table 12 Members of the Intelligence Community or System in each UNASUR Country (continued)					
Type of Intelligence Country	National Agency	Military Intelligence	Police Intelligence	Foreign Relations	Financial Intelligence
Chile	X	X	X		
Colombia	X	X	X		X
Ecuador	X	X	X		
Guyana		X	X		
Paraguay		X	X		
Peru	X	X	X	X	
Surinam		X	X		
Uruguay		X	X	X	X
Venezuela	X	X	X		

Source: Compiled by the author, 2013.

A third motive relates to the idea that all the countries of South America have experience in cooperation in at least one of the classic spheres of military, police, or strategic intelligence. All these countries, to a greater or lesser degree, engage in some form of intelligence cooperation, especially of the informal variety. Although this cooperation does not take place under the framework of UNASUR, its member countries all have experience in its practice.

In the realm of strategic intelligence, the Ibero-American Forum of Intelligence Service Directors meets periodically in various countries of the region.[494] Chile hosted the forum in 2003 in Viña del Mar. The forum reinforces the first two elements of the three-part knowledge-confidence-cooperation continuum that leads to intelligence cooperation.

For police intelligence, the Latin American and Caribbean Police Community (CLACIP) and the International Criminal Police Organization (INTERPOL) provide an impetus for intelligence cooperation among countries of the region through the direct exchange of information as well as through conferences, seminars, professional development courses, and the collaboration that goes

into producing documents that standardize certain police procedures.[495] Chile, for example, participates actively in these exchanges to the point of appointing officials specifically as liaison officers with these two groups. In particular, *Carabineros de Chile* and the *Policía de Investigaciones de Chile* engage with CLACIP and INTERPOL.

With respect to military intelligence, South American countries together with the United States participate in the South American Information Sharing Network (SURNET), underwritten by the U.S. Southern Command of the U.S. armed forces.[496] Similarly, various symposia or conferences have been held under the auspices of the U.S. Southern Command, where the chiefs of defense intelligence and invited specialists (to include some Europeans) have met to discuss regional intelligence initiatives. Chile hosted one of these meetings in 2011, with others in Brazil (2012), and Guatemala (2013).

Two additional multilateral organizations are active in South America. One is the South American Financial Action Group (GAFISUD), and the other the Regional Intelligence Liaison Office (RILO). The purpose of GAFISUD is

> to work toward the development and application of a worldwide strategy to combat money laundering and terrorist financing…. The effort includes support for the establishment of money laundering as a serious crime, the development of legal systems to investigate and judge those crimes, and the establishment of systems of notification about suspicious transactions and the promotion of reciprocal judicial assistance.[497]

GAFISUD aims to support the professional development of individuals involved in suppressing money laundering and to identify regional factors that need to be taken into account in applying measures against this phenomenon. South American GAFISUD members are: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, and Uruguay.[498]

The Regional Intelligence Liaison Office is

> a worldwide network for the exchange of information between and among custom's authorities everywhere, which

> brings together data related to illicit activities and which operates under the authority of the Worldwide Customs Organization.… It is also supported by the Customs Enforcement Network, which is an information system that provides information about the seizure of merchandise and controlled items from customs offices around the world.[499]

RILO maintains national points of contact in world regions where it is active. These exist in Argentina, Brazil, Bolivia, Colombia, Ecuador, Guyana, Paraguay, Peru, Uruguay, and Venezuela.

A fourth motive for intelligence cooperation derives from the experience in intelligence cooperation held by multilateral organizations that operate in distinct geographic regions, especially the Common Market of the South (MERCOSUR) and the Andean Community of Nations (CAN). In MERCOSUR, "an institutionalized mechanism for public security and criminal intelligence has been created."[500] It operates through

> opportunities and organizations within the Conference of Ministers of the Interior of MERCOSUR (RMI), where the implementation of a multinational group for criminal analysis has been discussed… although other than the existence of some informal mechanisms, permanent and institutionalized cooperation in intelligence in MERCOSUR and the expanded MERCOSUR has thus far been limited to counterterrorism intelligence, and to a lesser degree, some aspects of criminal intelligence. MERCOSUR has not yet created, even in the realm of criminal intelligence, an institutionalized mechanism to deal with organized crime.[501]

In the case of the Andean Community of Nations, intelligence cooperation "unlike in MERCOSUR, has taken place in an environment where public security and national defense have been conflated."[502] Ugarte explains that, as a result,

> intelligence cooperation within CAN has been organized around certain crimes, especially narcotrafficking and arms trafficking, with participation by the armed forces in some

> aspects of internal security and without the benefit of an institutional framework for intelligence cooperation.… This type of cooperation, in the absence of institutionalization and political control, evolved over time into region-wide application in the Latin American and Caribbean Police Intelligence Community (CLACIP) and the Police Community of America (AMERIPOL).[503]

There are advantages and disadvantages to the approach taken by CAN, but it is not the purpose of the current essay to evaluate this option, but rather to describe situations as observed.

Still, CLACIP-AMERIPOL

> could embody a sound basis for institutionalized cooperation in criminal intelligence in all the countries of Latin America and the Caribbean. If this cooperation does come about, it would be of inestimable value in the fight against organized crime. For this to occur would require that a formal treaty among the participating countries be signed, together with the creation of administrative organizations and a means of control. In this sense, the European Police Community (EUROPOL), an organization that AMERIPOL has sought in some ways to imitate, could be a suitable model.[504]

The possibility of intelligence cooperation becomes clear when one recognizes that Latin America and the Caribbean have "passed from the old, almost exclusively hemispheric approach to cooperation through increasingly subregional structures, and from the old style of cooperation based on the East-West conflict to intelligence cooperation based on public security."[505]

The following table indicates the likelihood that intelligence cooperation will emerge in each of the three realms we have examined. For defense and military intelligence, cooperation can develop under the auspices of the South American Defense Council (CDS) as it addresses cyberattacks, disaster assistance, and protection of natural resources, which are all established areas of interest. The CDS, in promoting defense cooperation, reinforces the possibility for an exchange of information among member countries. Information exchange

can take place in defense intelligence despite the lack of common security and defense policies in UNASUR. Those common policies may be a sufficient, but not necessary, condition for defense intelligence cooperation to occur. An additional possibility is for UNASUR to develop a common database that feeds on data supplied by member countries, that is then consulted by South American countries, and that is administered by the directors of defense intelligence from across the region, thereby replicating the SURNET model.

Table 13
Possibilities for Intelligence Cooperation in UNASUR

	Type of Intelligence		
Possibilities, according to the Treaty creating UNASUR	Military intelligence	Police information or criminal intelligence	Strategic intelligence
q) Coordination among specialized organizations of the member states	X	X	X
s) Exchange of information and experiences in the defense realm	X		
t) Cooperation in strengthening public security		X	
u) Sectorial cooperation as a mechanism for deepening South American integration	X	X	X

Source: Compiled by the author

Intelligence cooperation in military intelligence circles may be brought about through training courses, which can be extended to defense civilians, as well as through advanced courses in defense policy, which are already presented by the South American Defense Council. The courses would be especially helpful if they addressed intelligence not only as part of security studies, but also in terms of how the function is expressed in each of the UNASUR member countries.

At the same time, analytic techniques can be oriented to identifying and examining just what member states have in common, which in the South American Defense Council framework would translate to identifying common external

threats. The incorporation of intelligence as a phenomenon deserving of study, and as a focus of professional development, was debated in Colombia in 2012 during the regular meeting of UNASUR ministers of defense.

For police or criminal intelligence, cooperation may be mediated by UNASUR's South American Council for Public Security, Justice and Coordination of Actions against Transnational Organized Crime.[506]

Strategic intelligence cooperation can be brought about especially through regular, sponsored meetings of national intelligence service chiefs. The Ibero-American Forum of Intelligence Service Chiefs, as noted earlier, offers one possibility. This group meets to discuss topics of concern to the respective chiefs of state. Two themes commonly appear: specific problems in any one leader's country that affect other countries for which the impacts and possible conflict scenarios may need to be recognized and anticipated. In this light, several other states may be involved, which would validate the extension of cooperation to the multilateral sphere.

Still another spur to intelligence cooperation appears when potential participants learn how it may help them handle threat scenarios that arise outside the geographical space of South America, but that nonetheless may affect it seriously. Examples could include the economic crisis of the EU, the deceleration of Chinese growth, possible war between North and South Korea, effects of the Arab Spring, or a cyberattack against the critical infrastructure of some South American country or against one or more countries outside the region with which there is an important exchange of goods or services.[507]

One best practice found in the EU that may be replicated in the UNASUR region relates to the EU IntCen. This institution makes it possible to monitor events using the services of subject-matter experts from outside the intelligence services. The purpose of this institution within UNASUR would be to anticipate and detect potential regional crises, or international crises farther afield, that would benefit from a preventive approach. This approach may allow UNASUR members and a particular region to avoid a crisis, or at least bring thoughtful management to the conflict.

The reports generated by an intelligence center modeled on the EU IntCen could be supplied to all those responsible for strategic, police, or military

intelligence across the UNASUR region. The issues taken up by such a center would have been identified as of concern by heads of state, and it is to these individuals that an intelligence center would periodically report. The reports would also likely reach other specialized intelligence organizations.

Factors Affecting International Intelligence Cooperation

If at the present time, "institutionalized intelligence cooperation in support of international relations, international security and defense is at odds with diverse national interests, diverse ideas of security and defense, and persistent and important differences in foreign policy, even though it seems that these problems may be resolved in the medium term,"[508] then those factors that limit intelligence cooperation need to be addressed with the aim of promoting the institutionalization of intelligence cooperation as standard process. This essay will now explore these factors by referring to intelligence cooperation in a generic sense rather than in terms of any specific implementation by a country. However, some specifics will be examined in each important sphere of intelligence activity when those specifics are of particular relevance to the argument.

A lack of counterpart intelligence institutions in some pairs or sets of countries constitutes one limitation of intelligence cooperation. This situation amounts to having no interlocutors to facilitate communication, or to send or ask for data, information, or intelligence. It also impedes such tasks as carrying out a criminal investigation, conducting detailed intelligence analysis, or conducting a joint military operation.

Although most UNASUR countries do have intelligence organizations that cover the strategic, military, and police areas, some do not. This does not imply the total absence of some sphere of activity in any given country. However, intelligence cooperation becomes difficult when one country's coverage of strategic intelligence or police intelligence remains undeveloped. The fact that cooperation does occur throughout the region should incentivize all countries to upgrade deficient capabilities.

Each country in a potential cooperative network needs to have the capability to vet or confirm the validity of its own information, and to determine the reliability of the source. Otherwise, incorrect information may reduce others'

confidence in the originating state's contributions and further intelligence cooperation.

Ugarte suggests that "the traditional [intelligence] focus on another country and its intelligence capabilities as a probable enemy, even when it may also be an ally, makes cooperation difficult."[509] This scenario appears in some UNASUR member states that have experienced serious interstate conflict with neighbors. Nonetheless, most countries recognize the possibility of "more information being available than what one agency can collect by itself" and that "globalization has been an essential force in changing the nature of organized crime into a more transnational phenomenon."[510] Those considerations produce an immediate need to strengthen intelligence cooperation, even if common threats remain an insufficient condition to bring about cooperation.

Information received through intelligence cooperation cannot substitute for a country's own unique ability to collect information and generate intelligence for political leaders. However, the limited capabilities of any given country's own services justify international intelligence cooperation when additional information can confirm or deny hypotheses or scenarios about potentially dangerous situations.[511]

Institutionalization of the intelligence cooperation process depends on participant countries having passed through the knowledge-confidence-cooperation continuum. Informal intelligence cooperation does exist in both police and military spheres across South America. But it is cooperation without institutionalization, and "without the consolidation of an informal network, police intelligence will not be successful."[512] Intelligence cooperation becomes institutionalized when backed by a formal treaty signed by the president, ratified by the National Congress, and subjected to controls by government entities that operate independently of the organizations that engage in intelligence cooperation.[513]

If an elevated level of public corruption exists in a country, and/or there is a perception that it exists in the intelligence services, especially in the opinion of those in other national intelligence services, then international cooperation in intelligence will be low as a function of low confidence. The same outcome occurs when high personnel turnover afflicts an intelligence service. High

personnel turnover has occurred frequently in UNASUR countries and reduces the professionalism of individual practitioners and the service itself.[514]

Consolidating the Advantages of Intelligence Cooperation

Improving or deepening intelligence cooperation in the region requires a shift from informal to more formal, institutionalized relationships among agents and agencies. An institutionalization of cooperative processes offers certain benefits that lead to greater cooperation. It would bring a higher level of security to the exchange of information as record-keeping would require accountability for both sides in an exchange. The need to elevate the image and trustworthiness of an intelligence service among potential international partners would argue for improved training and education. These benefits of institutionalized cooperation should not overshadow or suppress benefits arising from informal contacts with counterpart services. That is, formalization of relationships and processes should not replace existing, informal exchanges of information, but rather complement and deepen those relationships.

As Ugarte points out, "the establishment of a formal and permanent mechanism for [intelligence] cooperation requires additional provisions for maintaining secrecy, the development of common classification standards and counterintelligence measures, and at least occasional meetings among liaison officers and other direct participants."[515] In the absence of any of these requirements, the extent of cooperation among UNASUR members will remain limited. Meanwhile, separate intelligence cooperation agreements among members will continue, but beyond the auspices of UNASUR.

South American countries do not yet have general agreements in place for intelligence cooperation under the UNASUR framework. The possibility has been discussed often in various meetings, but intelligence cooperation has not become part of the formal multilateral agenda. All member countries do field intelligence organizations, and they all have some experience in intelligence cooperation within the framework of other multilateral entities active in the region. To broaden and deepen intelligence cooperation will require overcoming a set of limitations, including especially the need to harmonize UNASUR members' foreign and defense policies, a task that remains for the future, but that remains achievable.

Conclusion

This study identifies four reasons to expect greater intelligence cooperation within the framework of the Union of South American Nations (UNASUR). The first motive arises from the fact that common threats to its members have been spelled out by UNASUR's Foundational Treaty. That most member countries have developed capabilities in police, military and strategic intelligence constitutes a second reason to expect greater cooperation. Another motive stems from the idea that member countries already have some experience with intelligence cooperation in multilateral organizations (RILO, GAFI and CLACIP). Finally, several member countries have gained experience in intelligence cooperation in support of public (citizen) security in the multilateral environments of MERCOSUR and the Andean Community of Nations. Taken together, these findings suggest that member countries are ready to move on to more formal intelligence cooperation within the framework of UNASUR.

Informal cooperation in intelligence does occur among intelligence organizations of most South American countries. Police intelligence cooperation exists in CLACIP, the Police Intelligence Community of Latin America and the Caribbean; and in the realm of strategic intelligence, it occurs in the meetings of the Forum for Directors of Ibero-American Intelligence. Military intelligence cooperation takes place across the region through the SURNET database administered by defense intelligence directors and the U.S. Southern Command. The ongoing identification of common threats by UNASUR members, together with police, military, and strategic intelligence cooperation (even if mainly on an informal basis), indicate that South American countries have a sound basis for advancing toward more formal intelligence cooperation within the UNASUR framework.

European Union experience demonstrates what is achievable in institutionalizing multilateral intelligence cooperation. A situation center following the European model could be appropriate and necessary for UNASUR. This center would, as in Europe, advise the highest national political authorities of UNASUR member countries and provide a place for the fusion of strategic, military, and police intelligence. Intelligence

cooperation could promote scenario analysis and crisis prevention for issues and areas where UNASUR may have strategic interests.

Educational institutions show promise in standardizing the professional development of intelligence specialists. Schools promote the consistent application of terms of practice and of analysis techniques, opening the way for future joint research and operations against organized criminal activity or common crimes.

The creation of interoperable databases will allow for real-time exchange of information on topics of mutual interest to specialists in the UNASUR countries. This will happen as member countries make progress along the three-part continuum of knowledge, confidence, and cooperation. Presently, multilateral intelligence operates at a point between the first and second elements of that range. The main limitation to progress in cooperation is a lack of confidence at both the personal and institutional levels. Low self-esteem among intelligence personnel coincides with frequent scandals, high turnover, and a stream of individuals who leave the services—including those who go to jail. These realities impede the development of the greater level of confidence needed to achieve cooperation.

Formal and informal cooperation in intelligence are distinct phenomena, and one should not be substituted for the other. Agreements that try to limit informal international contact between officials and services will reduce the overall level of cooperation because any coordination mechanism between services will be negatively affected by such strictures.

Informal cooperation may constitute a positive first step toward institutionalized cooperation between national intelligence officials as well as among senior UNASUR officials. The acceleration of intelligence cooperation in both areas would benefit from having the topic on the agenda of regional meetings. At this time, the weak initiatives in intelligence cooperation have not borne much fruit. Improved leadership can bring about the desirable results previewed in this essay.

Author's Biography

Carolina Sancho Hirane leads the intelligence program at the Chilean National Academy of Strategic and Political Studies in Santiago, where she offers courses at the undergraduate, graduate and postgraduate level. She has taught "Analysis of Contemporary International Conflict" at the School of Government and Public Administration of the University of Chile, as well as "Peace Process Construction" in the international relations curriculum of the University of Santiago de Chile. She holds the professional title of public administrator from the University of Chile's School of Government, with specialization in political science and public administration, and is a doctoral candidate with the University of Zaragoza (Spain). **Email:** *csanchohirane@yahoo.com.; csanchohirane@yahoo.es.*

Section Three
Intelligence Community Management of Privacy and Security Issues

Intelligence Community Management of Conflicting Privacy and Security Issues

Jose Manuel Ugarte

> "There are those employed in the intelligence security community of this country … who feel that they have a license to operate freely outside the dictates of law and otherwise to orchestrate as they see fit. Public officials at every level, whatever their position, like any other person, must respect and honor the Constitution and the laws of the United States."
>
> —Judge Barrington Parker[516]

Individual Rights, Privacy, and Intelligence

The essays in this section describe and assess the challenges to individual privacy that arise from the practice of intelligence. Intelligence practices naturally conflict with the enjoyment of individual rights. The nature of this conflict in a democratic state differs from that in a totalitarian environment, just as the practice of intelligence differs from one state to another.[517] As the author has noted elsewhere,[518] intelligence activity often contradicts the expectation that a democratic government will act transparently. Intelligence in fact seeks to eliminate a target's expectations of privacy.

The concepts of "bounded action" and "control" describe measures used to reduce or bridge the contradiction between maintaining government transparency and allowing instrusive intelligence. Intelligence and counterintelligence address threats from other states and from domestic organizations that wish to change the system of government through illegal means, or to threaten officials in their legitimate exercise of authority. In particular, a democratic state needs to bound or control the use of intelligence inside the country itself.

A democratic state demands legitimacy and efficacy from the institutions of government and should view the control of intelligence organizations and their activity as a natural consequence of that demand. The author believes that in a fully democratic system the protection of privacy does not conflict with the security interests of intelligence agencies. Intelligence professionals recognize in principle that their own actions can serve to protect the rights of individuals.

Appropriate controls or limits to intelligence activity offer the byproduct of protection of privacy. The constitutions of most states of the Americas recognize this idea, and article 11 of the American Convention on Human Rights establishes that "everyone has the right to have his honor respected and his dignity recognized" thereby avoiding "arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation." The Convention on Human Rights also specifies "the right to the protection of the law against such interference or attacks."[519] National legislation often includes additional measures to protect individual privacy beyond the protections afforded by controls and limitations over domestic intelligence actions.

Specific Bureaucratic Tools for the Protection of Individual Privacy

The protection of individual rights benefits from any country's requirement that certain intelligence actions be approved or disapproved by authorizing bodies. The requirements typically apply to the means and procedures for intercepting communications, whether by telephone, facsimile, or any means of voice or data transfer over distance, to include electronic mail. In addition, the requirements may apply to recording or any other form of acquiring private conversations, whether in a public setting or private dwelling. They usually extend to any means of pursuing or monitoring individuals. Naturally, these requirements apply only to the country's own intelligence services.

Control of intrusive means of collection chiefly aims to verify the reasons set forth by intelligence organizations for proceeding with the activity. If the collection is allowed to proceed, controls then ensure a minimal level of intrusiveness.[520] The judicial branch usually implements any controls over the monitoring of individuals. There are two variants of judicial control of intrusive intelligence actions. In the first, control is exercised by regular judges and courts, as in Canada and Argentina. The second arrangement involves special courts as set forth in U.S. Code, Title 50, Chapter 36, Subchapter I, §1803. This approach expedites the authorization of electronic surveillance for intelligence purposes, as set forth in the Foreign Intelligence Surveillance Act (FISA). In some countries, the authority to execute the interception of communications is given over to an intelligence agency itself. This is the approach

specified in Argentine Law 25520. In contrast, under Chile's Law 19974, the civilian intelligence agency (ANI) must make requests to intercept communications to the appropriate police agency, which executes the interception and then reports the results of the operation to the ANI director.[521]

Comprehensive or "organic" intelligence laws establish control over intelligence activity, but do not contain specific provisions for protecting the privacy of individuals. Examples include Brazilian Law 9883, Colombian Law 195/20,[522] Democratic Security Law 750 in Nicaragua,[523] and the Framework Law of the National Security System of Guatemala.[524] In the Brazilian case, the 1988 constitution contains a provision that guarantees the inviolability of communications, whereby only the judicial branch may intervene, and then only for purposes of criminal investigation or court proceedings, under procedures established in Law 9296 of 1996. This law limits communications interception to serious criminal cases, and occurs only under police jurisdiction. The interception of communications for intelligence purposes remains unaddressed by the Brazilian legal system.

Other intelligence laws across the region do establish guidelines for controlling the intrusiveness of intelligence activity, but they vary considerably in their level of specificity. Some may simply establish authorization requirements for the interception of "communications," as in the case of Argentine Law 25520. In contrast, Chilean Law 19974[525] requires authorization for "special procedures for obtaining information." It itemizes the collection of information from documents sent through the postal service and the use of electronic listening or recording (including audiovisual) devices. Surprisingly, the Chilean statute grants the heads of military and police intelligence services the power to use undercover agents and informants without judicial authorization. The Canadian Security and Intelligence Act establishes in great detail exactly what activity is subject to judicial authorization. Beyond required authorization for the interception of communications, the list includes obtaining any information, record, document, or anything at all as a result of search, entry, removal, examination, extraction, making copies, gaining access, or recording in any manner, or installing, maintaining, or removing anything, thereby covering definitively almost all possible means of undertaking intrusive actions.[526]

The protection of personal data from intelligence exploitation has yet to be addressed in Latin America. Intelligence laws generally do not include references to protecting personal data, even though most countries in the region have legal and constitutional ways of addressing the issue. Colombia's Law 195/2011 does have limited provisions for protection of personal data. The executive branch enforces its provisions, and individuals have no opportunity to correct, update, or delete personal data. Personal data receive much more comprehensive protection elsewhere.[527]

Commentary on the Essays in Part Three

Priscila Brandao

The essay by Priscila Carlos Brandao offers an analysis of issues surrounding the management of the Brazilian Intelligence System (SISBIN), and within SISBIN, the Public Security Intelligence Subsystem (SISP).

This essay addresses a reality common in the region: civilian intelligence agencies have wide-ranging domestic as well as foreign intelligence and counterintelligence powers. Brazil's agency (ABIN) bears the responsibility to produce all the knowledge necessary to advise the president of Brazil.[528] SISBIN—of which ABIN is the central agency—handles criminal intelligence (Brazil labels it "public security intelligence.") When the Intelligence System for Public Security (SISP) was created, ABIN became its (unsuitable) central agency as well. This was corrected when the National Secretariat of Public Security (SENASP-MJ) became the central agency for SISP. However, many agencies from outside the realm of public security remained in the SISP fold.

The SENASP-MJ created a Special Council for the Public Security Intelligence Subsystem (CE-SISP) for the purpose of developing norms for domestic intelligence activity. Again, council members were from intelligence organizations with little or no knowledge of public security or criminal intelligence.[529] Public-security intelligence organizations from individual Brazilian states and the Federal District were included as an afterthought, but did not have a vote in the council.[530]

The author also identifies the persistence of doctrinal concepts similar to those prevailing in the Cold War as another problem common to Latin America. Doctrinally, military intelligence agencies have several missions, among them

the maintenance of internal security. Even as police forces increasingly fight organized crime using a "criminal intelligence" approach, civilian and military intelligence agences have also ventured into this domain.[531]

Brandao draws attention to two other phenomena peculiar to the Brazilian intelligence system. One is the weakness of the General Coordinator of Intelligence (CGI). The CGI has few human resource and material capabilities with which to carry out its functions as a central office of the SISP. The second concerns the lack of specific legislation and rules to govern public security intelligence.

ABIN and armed forces opposition to developing intelligence doctrine for public security (even though it was ultimately adopted) demonstrates how civilian and military intelligence agencies in the region continue to push for keeping and even increasing their role in addressing organized crime. As a result, there is only a slow development of criminal intelligence by police authorities across Latin America. Only three countries, Argentina, Chile, and Guatemala, have criminal intelligence agencies. In Argentina, this agency is the National Office of Criminal Intelligence of the Argentine Federal Police and in Guatemala, the Directorate of Civilian Intelligence of the Ministry of the Interior.[532]

This rich essay illustrates the misapplication of intelligence methods, norms, and procedures—including an excessive use of information classification. The methods and procedures appropriate to national government or state intelligence are inappropriate for effective criminal intelligence.

The solution to the problems that Priscila Brandao points out will come through the development of criminal intelligence law and doctrine. The UK's National Intelligence Model (NIM) presents an interesting doctrinal innovation. The Association of Chiefs of Police of England and Wales developed the NIM doctrine specifically for police and public security activity.[533] Rather than encouraging compartmentalization and excessive classification, the NIM stimulates the exchange of information among participating police institutions. It accomplishes this on three levels: local, regional, and national-international and promotes the creation of standardized intelligence products as well as standard operating procedures. The success of the National

Intelligence Model has led to the formation, within EUROPOL, of a similar, European intelligence model.[534]

Liza Zuniga Collado

Liza Zuniga Collado suggests the need for "prison intelligence" in Chile and across the region. She also offers an analysis of legislative actions in Latin America that have yet to refer to prison intelligence.

Chile's Gendarmerie has the responsibility to monitor prisons and keep track of released prisoners.[535] Its Department of Prison Research and Analysis "studies and analyzes information about prison security." Additionally, it "collects and processes information on prison security for the purpose of supporting decisionmaking by prison authorities."[536]

Chilean practice combines prison intelligence with criminal intelligence. Soon after redesignating the Ministry of the Interior as the Ministry of the Interior and Public Security in 2011, Chile also created the Center for the Strategic Analysis of Crime (CEAD).[537] This criminal analysis[538] body[539] examines information generated by the leading institutional members of the penal system: the Gendarmerie of Chile, Carabineros of Chile, the Investigative Police, and the Public Prosecutor of the Justice Ministry. Their information populates the National Integrated Electronic Services Database, a Unified Criminal Information System. The system includes a National Public Security Observatory and an Office of Criminal Analysis with analysts from the Ministry of the Interior and Public Security, the Gendarmerie, Carabineros, and Investigative Police. This Office of Criminal Analysis carries out spatial, temporal, individual, and environmental analyses and explores criminal *modus operandi*. The identification of crime patterns and trends yields data for a new Unified Database of Criminal Information and facilitates the suppression and prevention of crime.

The Chilean prison service not only provides database information but also its own analysts, thereby fully participating in the creation and exploitation of criminal information. Something similar occurs in Argentina, where the Federal Prison Service has an intelligence organization, the Prison Intelligence Department, which submits information to the National Directorate of Criminal Intelligence, an intelligence agency assigned to produce criminal

intelligence. As this approach is taken up by other countries in the region, prison intelligence will become an important tool in the fight against crime.

Intelligence laws in the region do not address the role of prison intelligence. The intelligence laws of most other countries also do not, to the author's knowledge.[540] This is not to deny the importance of prison intelligence in the prevention of crime, or its role in ensuring adequate channels of communication between police and representatives of national or strategic intelligence. Intelligence legislation in the region does address both internal security and national defense issues. Attention to prison intelligence in the legislative process can advance public debate and lead to systematic improvements.[541]

Russell Swenson and Zulia Yanzadig Orozco Reynoso

This essay examines the effect of a country's intelligence activities on the rights of its individual citizens in the context of international intelligence cooperation and coordination. The essay analyzes an article by legal scholar Elizabeth Sepper.[542] Sepper warns of the negative consequences for human rights that emerge from autonomous decisionmaking by intelligence officials as they exchange information across national boundaries. She explains that this international exchange of information among intelligence officials has increased since September 11, 2001. She argues against the establishment of ties between the intelligence services of hegemonic countries and countries that may obtain inaccurate and unreliable information through torture. Sepper proposes various ways in which international law might reestablish control over intelligence agencies that engage in cooperation with their counterpart agencies around the world. She argues for establishing professional practices and ethical standards and for increasing international cooperation not in state or national intelligence, but in criminal intelligence.

Swenson and Orozco argue that international law has little coercive effect and that autonomy of decisionmaking within intelligence services exists as an inherent aspect of the activity. They also point out that international acculturation, or the transmission of behavioral norms by leading states, produces compliance with international behavioral norms.

In this reviewer's opinion, only limited control of international intelligence collaboration is possible because treaties or accords concerning intelligence

are state secrets and the intelligence obtained as a result of these agreements remains hidden from public view. If a country were to ignore these rules, not only would the interests of the originating country be placed in jeopardy, but the receiving country would be discredited as a trustworthy intelligence-sharing partner. The lack of a coercive effect in international law is not a central impediment to this problem of control. Each intelligence official is accountable to the laws of his own country in the exercise of his or her public function.[543] No legal immunity exists for intelligence officials' actions in their own country, or for their actions in a foreign country, unless they enjoy diplomatic immunity, or are covered by immunity agreements.

The present author shares Sepper's skepticism about the efficacy of transmitting the standards and norms of intelligence behavior from leading countries to those with which they interact, in particular with respect to the observance of human rights, even though standards and norms in other areas may be positively influenced. The interests of a country that needs additional intelligence tends to determine what intelligence activity is acceptable. The examples presented by Sepper speak eloquently of this truism.

Intelligence controls can be improved. In an important insight, Sepper notes that many countries with sophisticated intelligence controls have one or more intelligence organizations that continue to operate without effective controls, usually military intelligence organizations or other entities within a defense ministry. Although intelligence treaties or international memoranda of understanding cannot be made available to the public, treaties are subject to legislative ratification. These agreements need to be carefully debated in secret sessions of congress. Agreements not subject to legislative oversight need to be considered and probed by authorities who have internal and external oversight over intelligence practices.

The construction of an institutionalized, subregional environment for cooperation in criminal intelligence founded on the EUROPOL model, and able to address the diversity of challenges and needs of each subregion of Latin America, whether through UNASUR for South America, or in combination with a supporting organization at the hemispheric level, would constitute a basis for an effective effort against organized crime and terrorism in the region. Such a development in Latin America would contribute to overcoming

the risks of intelligence and information sharing and cooperation discussed by Sepper.

Jose Manuel Ugarte holds a doctorate from the *Universidad de Buenos Aires* (in administrative law), and serves as a specialist in administative law and public admistration at that university. He also serves as professor of administrative law at the *Universidad Católica de Santiago del Estero*. He teaches in the master's degree program of the *Universidad Abierta Interamericana*, and specializes in the field of defense management at the *Universidad Nacional de Tres de Febrero* and the Argentine *Escuela de Defensa Nacional*. **Email:** *manuguart@gmail.com.*

Comments on the Essays in Section Three

Thomas C. Bruneau

As anyone realizes who knows how intelligence agencies actually work in newer democracies, it is hard to be definitive about anything beyond their formal structures. In the absence of empirical data, these chapters seek to convey a certain sense of how the structures and processes of intelligence bureaucracy play out in Brazil, Chile, and Mexico.

The essay by Brandao demonstrates that although Brazil has been engaged in a decade-long effort to create a new intelligence system around the Brazilian Intelligence Agency (ABIN), the "system" remains redundant, overlapping, and opaque. The armed forces intelligence system survived and still has "a permanent internal security role" even though the National Information Service (SNI)—the intelligence arm of the military dictatorship that governed Brazil between 1964 and 1985—was eliminated in the early 1990s. As Brandao points out, ABIN does not have the legal authority to intercept phone calls or Internet communications, but must rely on the Federal Police for these fundamental sources of intelligence. In my view, this limitation greatly reduces the ABIN's effectiveness and may be a cause of unending scandals, as this agency tries to compensate for that lack of authority.

The chapter by Swenson and Orozco draws heavily on an article by Elizabeth Sepper in the *Texas International Law Journal* (Fall 2010). Sepper criticizes widespread, uncontrolled international intelligence sharing. The authors explore the context for intelligence sharing and the legal bases for certain intelligence activities. In terms of how intelligence can contribute to public security, they draw lessons mainly from the experience of Mexico. Looking more specifically at the Mexican Federal Police, they find that its competence and abilities, as a function of the resources made available to it, varies from state to state within that country, and that intelligence-based improvements to citizen security at the local level will depend on finding ethical ways to integrate national, even military, intelligence capabilities into preventive police action, perhaps even in advance of a nationwide legal framework for doing so.

The contribution by Zuniga argues for collecting intelligence in the prison environment as a legitimate, even if experimental, part of improving the

management of information-gathering practices in the national justice system. In reviewing the legal framework for intelligence activities in different countries, she finds that a weak legal basis for intelligence collection in Chile and the majority of the region's countries leaves much room for bureaucratic innovation. An accountable initiative in expanding the role of prison intelligence amounts to one such justifiable innovation.

What comes across in these three essays are several points that we at the Center for Civil-Military Relations have found to be common or typical in our work in several new democracies. These include the following: the need to rely on all imaginable sources of information to begin to say anything at all about the intelligence function; the absence of, or ambiguous, legal bases for the intelligence function; an unclear division of labor between different intelligence agencies, including between the military and civilian agencies; and ambiguity in who precisely does what, and to whom the final intelligence product is provided.

These studies also suggest that an additional challenge lies in how to define and measure the effectiveness of intelligence agencies. These are challenges that anyone interested in intelligence must deal with, although we may guess that it can never be accomplished in a very satisfying manner.

Thomas C. Bruneau serves as distinguished professor of national security affairs at the Naval Postgraduate School in Monterey, California, where he manges the program for Latin America and teaches short courses on intelligence reform for the Center for Civil-Military Relations. His most recent book, coedited with Cris Matei, is *The Routledge Handbook of Civil-Military Relations* (2012). **Email:** *tbruneau@nps.edu.*

Institutional Challenges in the Integration of the Brazilian Public Security Intelligence System

Priscila Carlos Brandao

This essay assesses a decade of work toward integrating the Public Security Intelligence Subsystem (SISP) into the larger Brazilian Intelligence System (SISBIN). An analysis of bureaucratic reform efforts and intelligence information handling inform the author's proposals to improve the difficult process of intelligence integration.

Intelligence Legitimacy and Efficacy in Brazil

Clear definitions of intelligence organizations and procedures can help an intelligence system govern itself, in the context of larger systems of which it it a part. Therefore, the definition of intelligence itself deserves close attention.[544] Although no confusion exists about the definition of intelligence in doctrinal terms, in practice Brazil's weak implementation of public security doctrine collides with a persistent military intelligence role in domestic security. The resulting bureaucratic uncertainties play a role in reducing the protection of basic civil rights as the government's involvement in public security increases.

The political and technical management of intelligence also depend on finding an operational definition acceptable to citizens and government officials alike. Although intelligence activity acquires its own "institutionality" and legitimacy as a state function, the definition of its goals remains a function of the political priorities of successive governments. Although intelligence serves the *state*, the particular *government* in power establishes its priorities. An intelligence plan serves as a guide to what actions may need to be undertaken. An efficacious plan has some degree of flexibility, in step with the typical uncertainties of intelligence.

As Brazilian strategic studies specialist Domicio Proença pointed out in a dialogue with the author, to govern intelligence we need to know what intelligence is, what it is for, whom it serves, what it costs, what protection it is accorded, the limits and controls to which it is subjected, and how it has been employed.[545] These issues cannot and should not be resolved independently

or even collectively by the agencies that make up the intelligence system. Instead, policies established in the political environment need to be reflected in each agency's goals and purposes.

Acknowledging that an intelligence system is governed from the outside does not diminish the importance of internal managers. They must have more than administrative knowledge: They need specific professional knowledge and an ability to manage resources and priorities effectively. Effective intelligence resource management meets sensible production deadlines and requires the joint effort of those who govern and those who manage. An ability to weigh what is politically satisfactory against what is professionally required helps to achieve this management ideal.[546]

Intelligence in the Public Security Domain

The political science debate surrounding the legitimacy of criminal (police) intelligence in the democratic context reflects widespread doubts about how to override or separate public security from public repression:

> As a key to ensuring governability, the formulation and implementation of policies established to handle the problems associated with public security should override the simple, reductionist view of security = police forces or security = repression, and instead embrace a common effort where security policies and criminal policies are conjoined in the social framework.[547]

The complexity of conducting internal intelligence activities needs to be made clear. Relevant international literature suggests that internal intelligence divides readily into two areas. First, security intelligence, or domestic intelligence, as it is known in the United States, identifies potential threats to the security of the state. Second, criminal intelligence, known in the United States as law enforcement intelligence (LEI), supports investigative police functions and the provision of public order and criminal justice. In Brazil, security intelligence and criminal intelligence are conflated in the definition of public security intelligence. More than a simple taxonomic issue, mixing the two reduces efficiency in the management of intelligence systems and intelligence performance.

In *Safety Has a Solution* (2006), Luiz Eduardo Soares diagnosed the state of public security in Brazil and identified two principal problems: weak management and obsolescent corporative structures.[548] He found that an enterprise management model would be necessary but insufficient to manage public security. Public security management also involves "knowing the problem that needs to be addressed; planning what is going to be done; evaluating what was done; identifying successes and failures, and monitoring the entire process."[549]

Soares points out why public security institutions require reform:

> Our police institutions are viscous and slow operations, not at all intelligent or creative; they do not value police personnel or prepare them adequately. They do not plan or evaluate what they do, they do not learn from their mistakes because they do not identify them, they are not familiar with the context of issues where they carry out their duties (policemen, individually, know very well; the police as an institution knows nothing). They do not cultivate the respect and confidence of the population ... they commit an immense number of crimes, when their task is to prevent crimes or to bring perpetrators to justice.[550]

Soares takes into account several factors: 1) managers of security organizations often have neither appropriate academic preparation nor knowledge in the administrative area; 2) administrative positions do not have a requirement for basic competence and trust; 3) public security institutions tend to be resistant to change; and 4) corporatist institutions do not cooperate; instead, rivalry and nasty disputes mark their relationships.[551]

Beyond the rivalry issue, Soares finds that structural problems also make institutional cooperation difficult. No standardized system of professional communication exists among agencies, which reduces data sharing for public security intelligence purposes. Each police force has its own way of training personnel with tailored courses; no common curriculum exists. Each police force also has its own way to classify information, making the interaction process more difficult. No national system organizes these institutions, which behave as isolated units and rarely cooperate. Even among the police forces

under the control of the Ministry of Justice—the Federal Police and the Transit Police—little dialogue exists. In light of this unruly scene, Soares asks: how could it be possible to create a professional culture in an efficient system, supported by a specialized, professional language that can be shared?[552]

Soares' concerns of 2006 remain valid today: how to bring a healthy process of change to the public security system in Brazil. Some needs include effective planning, professional development, systematic evaluation, ensuring that professionals are rewarded, and that procedures and control mechanisms themselves are evaluated. The present essay therefore asks: *What practical proposals for the intelligence field might address problems and strengthen reform and integration in public security information services?* This does not imply that reform is not possible or is not already underway, despite slow progress. Before offering some specific proposals, the essay will review the current institutional scene to find any evidence of consistent reform supportive of a less corporatist system.

Institutionalization of the Public Security Intelligence Subsystem

Brazil initiated its Public Security Intelligence Subsystem in 2000, with the civilian intelligence agency ABIN as the central agency for the system. ABIN held responsibility for foreign intelligence as well as internal intelligence. A dispute between the Ministry of Justice and the Institutional Security Cabinet about legal definitions of intelligence soon led to a new decree, which made the National Secretariat for Public Security of the Ministry of Justice the central institution.[553] Article 1 of the new decree required the Public Security Intelligence Subsystem "to co-ordinate and integrate all public-security intelligence activities across the country, as well as to support decisionmaking in federal and state governments with intelligence information." Articles 2 and 3 called on the Intelligence Subsystem's member organizations "to identify, follow and evaluate real or potential threats to public security and to produce knowledge and information in support of actions to neutralize and restrain criminal acts of any nature" (Article 2, §3). This vague guidance provided only a weak orientation to the subsequent debate about doctrinal and regulatory issues in public security intelligence.

As the central agency, the National Secretariat for Public Security oversaw the Federal Police and the Transit Police within the Justice Ministry; various

agencies of the Treasury department; of the Ministry of Regional Integration, and of the Ministry of Defense. Two agencies subordinated to the Institutional Security Cabinet, ABIN and National Anti-Drug Secretariat, also joined the circle. Additionally, the National Secretariat for Public Security presided over civilian and military police[554] of the 26 states and the Federal District—the relationship with military police being administered through mutual agreement.

In late 2001 the secretary of public security (whose office is responsible for the integration of intelligence operations) sponsored the first national seminar on public security intelligence.[555] Participants agreed that the Intelligence Subsystem provides *analytical* tools to identify the nature of criminal activity and to develop a profile of perpetrators and victims. The subsystem also assists in the solution of police investigations and *supports* public security planning and management by providing data, information, and knowledge.[556] Seminar participants found that few states have formal intelligence systems, reinforcing the need to adjust or standardize existing security structures. Professional personnel lack certain equipment needed to perform intelligence activities. Finally, the absence of public security doctrine contributes to inefficiencies in intelligence and counterintelligence.

With the placement of sociologist Luis Eduardo Soares as head of the Public Security Secretariat in 2003, some integration of public security intelligence occurred. He created the post of general coordinator of intelligence and improved the professional development of personnel.[557] In partnership with national subject-matter experts, the secretariat offered the first public security intelligence course oriented to the needs of state-level officials. The course offered professional tools with a sophisticated delivery.[558]

Praised by some, but criticized for its "academic orientation" by others, this initial course sowed the seeds for greater interaction, albeit informal, between the component agencies of the public security system. It led directly to the creation of the Criminal Intelligence Institute (INTECRIM) and the Brazilian Chapter of the International Association of Law Enforcement Intelligence Analysts (IALEIA). However, Soares' dramatic departure that same year and the new secretary's indifference to the course consigned it to near oblivion.[559]

During the tenure of Luiz Fernando Corrêa (2003/2007) as national secretary of public security, the development and approval of public security intelligence doctrine by the Intelligence Advisory Board proceeded slowly. Representatives of the states sought a legislative reform initiative that would fully involve the states in public security intelligence. Their initiative did move forward and received approval in April 2005.[560] However, it did not gain further political buy-in when presented to the Brazilian Congress as a modification of Law 3695. The low priority accorded intelligence then and now in political circles (notwithstanding that intelligence is presented as the solution to all the problems of public security) brought the further development of doctrine to a close.

Doctrine development ended at a critical stage—when the interaction of system members was up for discussion. To show a positive return on financial and political investment in two periods of debate, the general coordinator summarily ended the second phase of debate and approved the National Doctrine of Public Security Intelligence (DNISP) without an agreement to make it public. The third and final phase came with approval of the DNISP by the Special Advisory Council on 22 July 2009, under the purview of Secretary of Public Security Ricardo Balestreri.[561] Balestreri's tenure in the administration of Luiz Inacio Lula da Silva was marked by a political posture more explicitly "preventative" than that of his predecessor. This posture served to keep the office from being held hostage by any political pact among the states to further reform public security intelligence.

The Office of the General Intelligence Coordinator under Balestreri exhibited a penchant for political compromise and promoted an effective implementation of the new doctrine. Between 2008 and 2009 it transformed the criminal information database known as the National Information System for Justice and Public Security (INFOSEG) into the Network of National Integration of Information of Public Security (RENISP). Access to the revitalized network became easier with the use of encrypted pen drives. The General Intelligence Council during the Lula administration also created the National Council of Chiefs of Intelligence Agencies (CNCOI).[562] This move allowed greater state involvement in public security intelligence matters.

The General Intelligence Council has managed important steps toward institutionalization of the Intelligence Subsystem, although the results were less

than hoped for. Its policies for professional development and system integration were neglected as it coordinated security plans for the Soccer World Cup (2014) and the Olympic Games (2016).

Public Security Intelligence: Doctrine and Concept

Public security intelligence has the responsibility to provide accurate information for preventive police operations, street patrols, and criminal investigations.[563] However, an empirical challenge has been to understand that police intelligence produces knowledge rather than evidence of crimes. Intelligence documents are normally classified or highly restricted, and those who carry out intelligence are sworn to secrecy. Their information must be declassified to be used as evidence. Doing so carries the cost of revealing sources and methods or the identity of agents. Furthermore, differentiating the nature of and responsibility for pre- and post-crime intelligence remains an unresolved dilemma.

Despite the regulation of telephone tapping by Law 9296 (July 1996), police intelligence collection remained unregulated. Only with the approval of the National Public Security Intelligence Doctrine in 2009 did police intelligence collection have to take place within the scope of a criminal investigation. Police now may use special techniques to obtain nonpublic data with judicial pre-authorization, but only if there exist indications, evidence, or proof that someone has committed a crime.

Brazilian national legislation has not yet granted needed authority to public security agencies. In contrast to the Federal Bureau of Investigation in the United States, which after the September 11, 2001 attacks started to accumulate new and greater domestic intelligence and criminal intelligence capabilities,[564] the Brazilian Federal Police and ABIN do not have the authority to collect and analyze information from intelligence penetration of suspected terrorist groups in the country. The Federal Police can only take intelligence measures after a crime such as arms trafficking or money laundering has occurred. The principles of legitimacy and proportionality support a proactive counterintelligence capability in Brazil. The continuing absence or insufficiency of intelligence authority explains military and ABIN reluctance to support the creation of a specific doctrine dedicated to public security intelligence.

In contrast with these restrictions on civilian or federal police intelligence activity, the Brazilian Constitution specifies that the military can act in defense of law and order as a secondary mission. The military's concept of "internal enemy" still influences the performance of military intelligence activities. Although internal security is not part of current defense policy, civilian governments have made little effort to clarify which situations or actors should be defined as threats, or to establish the difference between internal defense, security, and defense of the rule of law.

The defined roles of the Ministry of Defense range from policing the borders, guaranteeing order, and providing public and national defense, to guaranteeing electoral process and civil defense. The breadth of these roles dilutes the ability of military intelligence to carry out its function, since its human, technological, and budgetary resources are far less than needed.[565] At the same time, the various expectations make the military services a flexible agent when the state cannot carry out its goals through other agencies.

Chapter XVI of Regulation 7364/10 assigns the armed forces the responsibility to enforce law and order "when appropriate." The regulation aims to preserve public order, protect the civilian electoral system, promote national development and civil defense, combat crime in the border regions, and ensure the integrity of the natural environment.[566] The military services ignore the "when appropriate" caveat in favor of the more expedient "upon the initiative of any of the military services." They interpret the regulation as granting a permanent internal security role to the armed forces.

The chief tenet of the old National Security Doctrine was that confict is continuous. This view of conflict has persisted in the military organizations as part of the logic of state security, to the detriment of personal or public security. The prestigious and widely read magazine *Carta Capital* divulged (October 19, 2011) excerpts of a document titled "Campaign Manual—Counterintelligence." It reveals unequivocal evidence of this military mentality as it shows how linguistic expressions are manipulated to legitimize and justify military action in the internal sphere. A counterintelligence manual can be a good thing, given the presence of pseudo-nongovernment organizations that engage in biopiracy and other pernicious crimes. But the manual's definition of "adversarial elements" raises questions:

> Social groups and movements, non-governmental organizations, and *even* governmental bodies, of an ideological nature or not—acting in the country and the exterior—or independent actors, radical elements or those associated with them, who defend radical and revolutionary changes, *exceeding*, in their political-ideological, religious or ethnic character, the limits of institutional legality within the democratic Rule of Law, and *whose illegal procedures can come to compromise public order and even the internal order of the country*.[567]

The manual's language legitimizes armed forces actions when internal adversarial forces exceed the limits of institutional legality, or when their actions compromise public order. In doing so, it clearly ignores the principle of proportionality. By these guidelines, the actions of the Landless Movement (*Movimento dos sem Terra*) or strike actions by Post Office laborers cannot be handled by the largely civilian public security agencies. One must ask why these actors would be monitored even by civilian intelligence agencies in a country operating under democratic rule of law. Intolerance of adversarial opinions characterizes an authoritarian state, and the application of policies reflecting the National Security Doctrine leads to inappropriate management choices in the security and defense realm.[568]

When Brazilian armed forces prioritize internal security, they expend their power on a secondary mission. This approach undermines the otherwise steady growth of Brazilian influence on the international scene. The country does need an intelligence doctrine that will enable it to address foreign espionage and terrorism (a phenomenon distinct from the military concept of subversion).[569]

Police Intelligence and Public Security

The legal rules concerning the admissibility of evidence apply to investigative intelligence analysis as well as to police inquiry. Police intelligence produces knowledge that confirms evidence, certifies indications, or substantiates the results of tests to identify perpetrators of crime. Yet its work is not confined to the investigation of evidence. Police intelligence analysis participates in an information feedback system that unleashes a cyclical process of knowledge production. From the moment new information is collected and new analyses

are produced, the probability of new investigations increases, successively transforming investigative analysis into strategic analysis. According to Monica Lacerda, "the product of the analytical process is combined into a database and is used to forecast and prevent undesirable events, in this way acting not so much as investigative, but preventive, police intelligence."[570]

Public security officers do not have clear guidelines for the admissibility of evidence from intrusive searches for denied data. Uniformed officers rather than investigative police sometimes engage in preventive public security intelligence operations focused on crimes and serious disturbances of the public order at the strategic level. This creates a problem because uniformed officers train only for tactical or operational situations. This problem also affects police operations in noncriminal environments where public security managers have to make a variety of autonomous decisions without the benefit of clear rules.

The effective management of public security intelligence rests on restraining the use of intrusive methods and improving the capabilities of analysts. A positive step in that direction depends on maximizing the production of intelligence based on open sources and creating accessible, well-organized databases.

Practical Proposals for Intelligence-Based Public Security Reform

Public security intelligence managers in Brazil have the opportunity to improve performance by institutionalizing informal exchanges of information among different agents and agencies. Informal exchanges already take place on an everyday basis in public security agencies of all types.

In *The Blue Planet*, Michael Bayer shows why a failure to capitalize on informal exchanges of data between police agencies across the world degrades the worldwide campaign against terrorism: "formal relationships are helpful, informal relationships are powerful."[571] According to the author, certain characteristics inherent to police agencies make them a powerful instrument against complex crime and, by extension, against terrorism: 1) police have the ability to adapt, adjust, and act quickly, in the sense of finding answers to issues or situations that demand immediate action[572]; 2) a feeling of

fellowship or belonging exists between police agencies, because they have a common mission—maintenance of law and order—and common enemies—criminals—as a stimulus (Bayer sees the positive side of police allegiance, the "culture of the badge," as the factor promoting cooperation between similar agencies)[573]; 3) the capillarity of police agencies adds another positive factor. Capillarity allows policemen to act at the various levels (state, federal, local), and in the widest variety of places (metropolises, villages, boroughs, ghettos). Police cooperation transcends religions, ethnicities, political preferences, and other dividing factors that could make cooperation impracticable. Capillarity drives the interaction described in *The Blue Planet*. Investigative "know-how" combined with informal contacts give police an unrivaled capacity "to connect the dots"[574]; 4) police possess independence in relation to centers of power. This distinguishes police from intelligence services, which are themselves agencies of power in governments. Political independence allows the autonomy necessary for police to carry out missions of any kind.[575]

These factors represent a set of necessary conditions for the exchange of information, but are not sufficient to make it happen. A smooth exchange of information between police and among their agencies requires mutual confidence as the basis for any circulation of information. According to Bayer, two factors promote confidence: a feeling of belonging, and reciprocity.[576] In order for information to circulate informally, either preliminary contact between individuals in different agencies must have already occurred, or a well-founded expectation exists that a policeman can count on help when needed—an officer will always help his colleague.

Why should data exchange occur on an informal basis? First, information from informal sources enriches data already available in bureaucratic channels. Second, slow bureaucratic information exchange reduces the necessary agility of police agencies. When information sharing takes place in a formal environment, it has to be written down, transmitted, registered, analyzed, debated, evaluated, approved or disapproved over days, weeks, or months. The exchange of information between police officers, done "cop you cop," can take only minutes—the time for a phone call or fax.

Bayer's findings address the informal interactions between agencies of different countries—agencies that do not compete directly for power, budget or influence. Such interaction can serve as a behavioral goal for Brazilian

police agencies and as a reference point for the establishment of an extensive police network for gathering data of certain types—what Bayer labels a "dragnet." Police as well as intelligence officials in Brazil know the value and importance of compiling and having access to certain databases; that is, they are aware of the need for a multidirectional flow of information. However, various factors keep police agencies from cooperating with each other. Bureaucratric turf battles, a negative aspect of corporatism, detracts from the ideal of cooperation.

To understand the potential for greater information exchange in the Brazilian public security system, one must address two questions: Who encourages and controls the circulation of information, and what information can be shared? The National Secretariat for Public Security bears the responsibility to integrate the work of Public Security Intelligence Subsystem organizations. It already coordinates the system of intelligence information exchange known as the National Public Security Information Network. However, exchanges on this network obey a formal logic, guided by a doctrine that regulates requests for information, guides the creation of Relints (intelligence reports), and imposes dissemination restrictions on classified information. The associated lack of agility calls for the development of new intelligence architecture whereby agencies that wish to share sensitive information would have that information validated and approved for exchange rapidly under the auspices of a unique protocol.

Bayer finds that a culture of over-classification of information inhibits the exchange of information for public security purposes. This remnant of Cold War thinking feeds intelligence agency turf wars. Further, when information becomes classified, interest in it increases, along with its overall vulnerability to disclosure.[577] Brazilian classification rules apply specifically to investigatory information or intelligence related to crime prevention or reduction.[578] But how can one determine which information related to criminal conduct realistically needs to be classified, and which may be circulated to other agencies for legitimate purposes? Bayer suggests that information not be classified without a concrete probability that disclosure of the knowledge would damage national security.[579] Although the term "national security" remains nebulous, information should not be classified to: a) cover up a violation of the law, an error, or administrative inefficiency; b) prevent discomfort to a

person, organization, or agency; c) reduce competition between agencies; or d) prevent or delay the release of information that does not require protection in the interest of national security.[580] Bayer further suggests that a "sensitive but unclassified information" label for police intelligence data would stimulate more *secure* transmission of data. The risk of such information being leaked to the public is low because criminal information is protected from disclosure by criminal law.[581]

Public Security Intelligence Subsystem administrators can develop training courses to foment a culture of organizing and sharing public security information through accessible databases. Students from a wide variety of public security organizations would find colleagues with whom to develop personal ties and the mutual confidence conducive to information sharing for crime prevention and resolution.

Assessment and Forecast

How well integrated is Brazil's Public Security Intelligence Subsystem? The chief integrating mechanism, the 2009 National Doctrine for Public Security Intelligence, has yet to be fully implemented. The doctrine has not yet been fully implemented even in the federal police force.[582] Standardization of language and procedures would coincide with the adoption of integrative concepts and values such as information sharing. Working-level cooperation does not take place among the public security intelligence systems of the individual Brazilian states, either formally or informally through social networks. The continuing lack of a common professional vocabulary suggests the absence of management interest in promoting interaction between the corporative agencies that make up the subsystem. Brazil lacks a good understanding of the role of its basic public security intelligence components, undermining any suggestion for appropriate political actions and resource management decisions to improve its integration in line with democratic principles.

The standardization of concepts and techniques for public security intelligence does not by itself guarantee the capillarity or integration of the subsystem. A broader dissemination of information and intelligence products requires mutual trust and a commitment to change the culture of information classification among multiple agencies. Recent international experience demonstrates that the useful sharing of sensitive information can occur in a

formal manner as well as through informal but professional social networks. Regardless of the route chosen, knowing who is to produce information and what particular expressions mean, as well as instilling confidence among the security institutions, are minimum requirements to ensure that information exchange does occur.

The Public Security Intelligence Subsystem, created in 2000, has not been able to facilitate the desired interaction between and among its distinct, corporatist organizations. Among the challenges identified by intelligence managers and operators in the period immediately following the creation of the subsystem,[583] most remain to be addressed: designation of appropriate authority, professional development, efficient management, standardization, and cooperation. Only two of the problems initially identified have been cured: new doctrine has been created and approved, and an internal communications network has been put in place, capable of safely transmitting classified information. The National Network for Public Security Information, created with the intention of meeting this need, is not yet widely used. Where a lack of trust and cooperation still reign, personal and informal solutions are still seen as the best option.

Despite the ongoing, popular discussion of the need to produce more and better information on crimes and criminals, Brazil has yet to achieve the specialization and expertise to generate what in other countries is called intelligence-led policing.[584] The production of knowledge in police work, as well as in the criminal system, in the broad sense, depends on the synergy among technological gains made possible by information technology and communications infrastructure, the quality of information databases, and the wealth of information embodied in operational activity itself (both preventive and investigative).

The development of a system of public security intelligence in Brazil requires a careful review of its activity by public security stewards. They need better knowledge of how the system operates, and they need to promote its integration, attitudes toward cooperation, professional development, and especially an unpretentiousness among managers so as to preserve advances already made. Beyond the existing public security intelligence doctrine, generating a more comprehensive national intelligence policy should be the country's highest priority.

Brazil also requires a review of the legal mechanisms regulating the collection of intelligence information by the police as well as by other national intelligence agencies. The Brazilian civilian intelligence agency, ABIN, does not have authority to intercept communications of any type. If an intelligence system expects to deal with hard targets and obtain protected or denied information, how can the chief strategic intelligence agency not have the authority to carry out standard intelligence and counterintelligence functions? Table 14 suggests some current answers to that question and recommendations for improving management efficiency.

Table 14
Schematic Synthesis of Suggestions for National Intelligence Improvement

Criterion for Efficacy	Current Situation	Suggestions
Establish clear definition of the concept of intelligence, widely understood and accepted by those whom it serves.	Conceptual ambiguity	Specify the relevant arenas for intelligence action (defense, public security, international relations), delimiting the areas of responsibility for each component of the intelligence community.
Define who governs (oversees), who manages, who executes, and how governance is to be done.	Ambiguity over the roles of civilian, military, and police in the production of knowledge: threat to privacy and other civil rights	Define the specialty of each organization in the intelligence system, taking into account its essence, its place in the system, and its purpose.
Spell out how each aspect of intelligence governance will be handled: planning, professional development, evaluation and assessment of professionals.	Waiting for the construction and approval of a national intelligence policy	Approval of the national intelligence policy, to guide planning and set goals for each organization in line with policy objectives.

Table 14
Schematic Synthesis of Suggestions for National Intelligence Improvement (continued)

Criterion for Efficacy	Current Situation	Suggestions
Standardization	Waiting for the public release of the National Doctrine for Public Security Intelligence	Arrange meetings, create applied academic courses to promote greater interaction among intelligence community organizations, and standardize terminology.
Efficient management	Errors are not corrected because they are not detected; absence of effective communication between "castes" in the intelligence service.	Heal the fracture between intelligence operators (who know a lot) and managers, with whom operators do not often exchange ideas.
Information sharing	Exclusive corporate or private custody of information	a) Institutionalize informal procedures for information exchange through increased personal interaction among colleagues (can be accomplished by the National Secretary of Public Security through security protocols); b) Promote a culture of information sharing to reduce hoarding.

Source: Compiled by the author.

Author's Biography

Priscila Brandao holds a Ph.D. in social sciences from the State University of Campinas (2005), and has done postdoctoral work in governance and governability in counterdrug trafficking (U.S. National Defense University) and in intelligence professionalization (University of Burgos/Spain). Since January 2006 she has served as adjunct professor at the Federal University of Minas Gerais (UFMG). She specializes in history, with an emphasis on contemporary political institutions, and has interests in military dictatorship, intelligence community affairs, the Brazilian civilian intelligence agency, and criminal intelligence in Latin America. She serves as a consultant to the federal government and some state governments in the area of criminal intelligence and heads the research division of the National Council of Scientific and Technological Development—governmental intelligence. She is also the coordinating director of the UFMG Center for Strategic Studies of Government Intelligence. Her publications include *SNI and ABIN* (Rio De Janeiro: EDFGV, 2002) and *Secret Services and Democracy* (Niterói: Impetus Publishing Company, 2010). For her complete resume see: *http://lattes.cnpq.br/5546418263728807.*

Intelligence—from the Prison Environment to the National Security System

Liza Zuniga Collado

Introduction

Why should a country develop intelligence in a prison environment? Why would prison intelligence have strategic value? How can one manage intelligence activity in this environment? These questions shape the following examination of two public security areas—prisons and intelligence. These seemingly unrelated realms are linked by the emerging role of intelligence in public security. Although routine use of the intelligence function in national incarceration systems remains for the future, opportunities for its development already exist in various Latin American countries. The ideas presented here aim to promote a debate about the simultaneous management of prisons and intelligence.

One can begin to answer these introductory questions by recognizing the implications of security system reform in the 1970s. In those years a set of related security organizations, each operating in its own sphere of competence but also cooperating with others in the network, came to embody the "security system" concept. In this network, minimal but vital coordination among organizations would allow for the maturation of each security institution in complementary fashion. Presently, prison systems often function as a set of "human containers"—isolated places designed to carry out criminal policies and judicial decisions. This essay applies the decades-old, collaborative security system idea to argue for the maturation of prison systems through their adoption of an intelligence function linking incarceration institutions with other elements of a state's overall security system.

Latin American intelligence systems depend on laws (see Table 2), official definitions of their activities, and a variety of organizations to carry out a central function of any national security system. Countries of the region fall into two groups: 1) those that have been able to discuss and enact intelligence laws and develop intelligence communities; adopt ethical principles of conduct; arrange for external oversight to limit and control intelligence activity; and collaborate with a network of organizations from different areas of society;

and 2) a second group of countries that shows little or no tendency to adopt those measures. All countries of the region do have in common the persistent concept of intelligence as a strategic or political function, as a military specialty, and as a police tool.

This essay discusses the preconditions that might allow for or encourage the development of prison intelligence. A crisis environment in the prison systems of the region makes the insertion of intelligence capabilities in these institutions a difficult proposition. However, the addition of an intelligence capability would give prison administrators an opportunity to integrate their operations with the national security system, a long-postponed administrative goal. The idea of integrating intelligence services with the prison system may seem ambitious in view of the precarious state of prisons in the region. It will be possible to do so to only as the prison system begins to overcome multiple deficiencies.

Cooperation as the Basis for a Multidimensional Security System

Holistic security systems emerged in Eastern Europe in the 1990s, as countries in that region responded to the need for reform and reorganization of their security institutions. The idea of a holistic system applies to other contexts as well. Countries undergoing rapid development or that have reached full development apply the concept as a means of improving the quality of their institutions. The need for political reconfiguration in Latin America differs from that in Eastern Europe because each region has experienced distinct types of conflict. Latin America has undertaken a series of post-dictator military reforms in a "third wave of democratization." The majority of these reforms aim to reestablish civilian political leadership over the armed forces and to separate police work from military duties, making both these institutions compliant rather than deliberative bodies.[585] Some security elements, including judicial reform, remained unaddressed in early reform efforts. Thus, prison services in the last two decades have suffered the results of increasingly punitive criminal policies. Longer sentences and more crimes of record, without the counterweight of an incarceration policy for the prison system, deprive more inmates of their freedom. Prisons receive more prisoners, some of them violent offenders from organized crime groups, but not the additional

personnel or infrastructure to handle the inmate population. This situation holds across all of Latin America with subtle differences from place to place.

The Organization for Economic Cooperation and Development's (OECD) broad concept of national and public security helps answer why prison services should be incorporated fully into a country's security system. The OECD finds that "the security of people and the security of states are mutually reinforcing. A wide range of state institutions and other entities may be responsible for ensuring some aspect of security." For the OECD, the "security sector" includes

> all the actors, their roles, responsibilities and actions—working together to manage and operate the system in a manner that is more consistent with democratic norms and sound principles of good governance, and thus contributes to a well-functioning security framework.[586]

From this definition there follow two reasons to incorporate prison administration into the security sector. The first is that *all the actors* are to be included, whether they be primary actors (such as the armed forces, the police, the intelligence services), actors of an administrative or oversight nature (ministries, legislative committees, financial administrators), actors associated with the administration of justice (penal institutions, courts, human rights commissions) or nonstate actors (such as private security services). The system of incarceration constitutes a part of the sector, although not as a central actor in the same way as the armed forces or police. The second element justifying the incorporation of prison administration into the security sector is that a security system contributes to *good governance* and to accomplishing daily security objectives. This suggests that the security sector contributes to a country's governability, as security permits the development of broad human capabilities in a society.

The concept of governability has been developed and defined in security terms by the Inter-American Commission on Human Rights: democratic governability in public security (*seguridad ciudadana*) terms is the institutional ability on the part of legitimate authorities to design, implement, and evaluate policies for the prevention and control of crime and violence.[587] Three points about governability should be highlighted: 1) the concept assumes

a democratic system, where civil authorities are in office as a result of free elections; 2) it focuses on the idea of public security; that is, security that goes beyond that provided by the traditional services such as the police, and implies for citizens a more holistic concept of security; and 3) the concept also implies the employment of preventive measures, to go along with the traditional prosecutorial approach. The last point is particularly important in the prison environment. Although the penal system seeks to control those who have already broken the law, preventive policies and tools remain appropriate as a way to reduce recidivism.

Even as Latin America has moved toward adequate public security policies with community participation, has adopted prevention programs of all types, and has undertaken police reforms, its prisons have remained essentially unchanged. A few improvements have come from individual efforts and isolated programs. Police and judicial establishments do not consider prison administration an equal player in the criminal justice system. Prison administrators are viewed as "jailkeepers" and not professional justice employees.[588] Another reason for the neglect of prison personnel is that governments do not benefit politically from demonstrating that they are capable of developing an incarceration system that respects human rights. Decisionmakers believe that sending more people to prison, without considering what takes place within the institution, remains the best way to respond to citizen demands for greater security. This approach has acquired the label "punitive populism."[589]

Latin America has adopted the concept of human security as a part of multidimensional security, whereby security institutions exist within a system. The origin of this thinking about security in multidimensional terms lies in the Organization of American States' (OAS) Declaration on Security in the Americas (2003), which maintains that

> security in the Hemisphere is multidimensional by nature and encompasses traditional as well as new threats, concerns, and other challenges to the security and the priorities of the States. Security contributes to the consolidation of peace, integrated development and social justice, and is based on democratic values, respect, the promotion and defense of human rights, solidarity, cooperation, and respect for national sovereignty.[590]

This regionally accepted concept bears similarities to the idea of human security promoted by the United Nations Development Project (UNDP), and in particular by the governments of Canada and Japan, at the beginning of the 1990s. The UNDP concept focuses on individuals and on integrative tendencies and multidimensional themes in public affairs. It emphasizes multilateralism and cooperation in the security dimension as well as in other areas of development.[591]

If security has multiple dimensions, and if the threats we face are themselves of diverse origins, then the organizations charged with confronting these threats also need to be diverse and multiple. A country cannot rely only on only one or two institutions to protect its people. Prisons address both common and organized delinquency, and can develop intelligence not only about inmates, but also about the leadership and operation of their criminal organizations. Intelligence can contribute to improving the management of prisons by providing the unique data to help administrators make optimal use of all existing information. Intelligence information allows prison administrators to improve their own security and gives them insights to share with other elements of the security community. In this way, administrators can move from a passive to a more active role in the national security system.

The Intelligence Function and the Prison Environment

Strategic intelligence provides information for decisonmaking and for planning. The intelligence production process itself requires planning and development of systems and methods to collect information and to administer the intelligence organization itself. The same planning process applies to many security environments, although strategic intelligence has principally been associated with national defense. Today, the business world incorporates and applies the principles of intelligence production, and correspondingly, an intelligence community now needs to include economic and social issues in its purview to protect a country's citizens.

Intelligence treats criminal behavior as a social phenomenon with security implications. Intelligence analysis thus enables a society to address this dynamic phenomenon through strategic planning. Such planning can guide preventive actions by police and social workers to address offenders who constantly seek new avenues of criminal advantage. The United States first employed

intelligence capabilities in the 1950s and 1960s to monitor gang activity that directly challenged the security of penal institutions. Prison officials slowly developed trained groups to carry out monitoring as an intelligence activity.[592] Today, the coordinated efforts of criminal gangs within the prison establishment—especially evident in Central America—signal the increasing need for intelligence monitoring within these institutions.

Most police organizations in Latin America now incorporate intelligence capabilities directly in small, specialized units, as a formal division of police organizations, or indirectly through crime prevention and investigation units. In contrast, prison administrators have typically not yet incorporated intelligence into their repertoire of security tools. They limit themselves to maintaining control over inmates or managing programs for reinserting prisoners back into society. Prison intelligence remains an area of public administration lacking empirical research, and therefore decisions regarding its use rest on generalizations reported in the press. The lack of empirical research contributes to the considerable differences that exist between the real experience of prison life and what is popularly imagined. A problem arises when decision-makers have access only to the imagined reality.

Intelligence capabilities should be employed in the prison environment for two reasons. First, when prison administrators coordinate with other security institutions, the security system gains governability and effectiveness. The contribution of prison administrators to a country's security comes from their having custody of the inmate population. The social dynamics among this population reveal power relationships and provide indicators of disorder and conflict.[593] Prison personnel serve as the eyes and ears of intelligence analysts because of their daily contact with prisoners.[594] Although a prison is the most powerful symbol of the state's power to punish, at the same time it exists as proof that the state has failed to include all citizens in an integrated body politic. This fact makes it indispensable to consider prisons an integral part of a country's security institutions. No better place exists to observe the social interactions that might inform the development of public policies suited to the control and reduction of criminal groups.

The second reason for adding an intelligence component to the prison environment comes from its utility in administering the facility. Intelligence contributes to planning future actions, making changes in policies, and

anticipating events (such as riots and escape attempts) that might threaten security within the institution. Prison personnel require adequate training to keep a watchful eye on inmates. Informal arrangements between prison personnel and inmates can be a good source of information and can also help to maintain order in the facility. These arrangements can alleviate tensions, reduce imperfections in procedures, keep the most disruptive prisoners under control, and reinforce the status of leaders among the inmate population.[595] Systematic collection, evaluation, and analysis of information makes intelligence well suited to the prison environment, where decisions by administrators have a direct effect on the security of prisoners and employees. Intelligence has value beyond the institution as well, in monitoring, identifying, and documenting information about gang members or criminal organizations and collaborating with external officials, whether police or other justice officials.

Intelligence Legislation and the Opportunity to Build an Integrated Security System

A state's monopoly on the use of force allows it to defend against external and internal threats, maintain public order, and provide justice for citizens. The effectiveness of each of these functions depends on the intelligence function. The judicial branch has the opportunity to exercise control over intelligence—deciding, for example, the appropriateness of particular means of information collection. Judicial branch organizations that administer prisons can also *produce* intelligence. It is erroneous to consider the judicial branch as an entity concerned only with the control and oversight of intelligence. Some countries have corrected that error through intelligence legislation.[596]

Across the region, some intelligence laws are more complete than others. The more comprehensive laws include basic definitions and an indication of what institutions make up the intelligence system, their respective roles in the system, and a description of control and oversight mechanisms (see Table 3). In some other countries of the region, executive orders or decrees refer to an intelligence community but do not go beyond that nominal level of attention.

In Argentina, article 13 of intelligence Law 25520 (2001) stipulates that the Intelligence Secretariat can "[r]equire all the organizations of the Executive Branch to share the information needed to carry out its functions." This

provision promotes the exchange of information and intelligence between officials of the prison system and the national intelligence system of Argentina. Nearly a decade later, Argentina's National Security Ministry was assigned "to deal with the production of intelligence and information that is [also] the business of armed forces and the police."[597] That is, this ministry itself has a role, together with the police whose work they coordinate, in carrying out intelligence activity. The internal security system thus coordinates all judicial branch activity, but the law fails to specify coordination with the prison system at the national or provincial level.

Chile's Law 19974 (2004) establishing the National Intelligence Agency (ANI) also failed to mention the participation of the *Gendarmeria* (the organization charged with the administration of prisons) in the set of institutions that make up the national intelligence system. As in Argentina, the law addresses military, strategic, and criminal intelligence—the latter the responsibility of the forces of order and security; that is, the police. Additionally, the law declares that the ANI may require that the Gendarmeria share information related to ANI activities, and the Gendarmeria must comply with the request. Criminal intelligence, understood as "police intelligence," "includes the processing of information related to the actions of individuals, groups, and organizations that in any manner affects or can affect public order and internal public security" (article 22 of Law 19974). These organizations or groups often continue operating from within prisons, and therefore the Gendarmeria can contribute continuously as a formal and direct part of the national security system, and not just when the ANI demands it. If the Gendarmeria were to carry out intelligence in an institutionalized fashion, it could make a substantive contribution to the national security system. This possibility is specifically mentioned in the 2004 law.

The Brazilian Intelligence Agency (ABIN), attached to the office of the president of the republic, is to "plan, carry out, coordinate, supervise, and control intelligence activities of the government" (article 3 of Law 9833 [1999]). This law specifies that any federal governmental organization that directly or indirectly produces knowledge of interest to intelligence, and especially those entities responsible for external defense, internal security, and international relations, will be part of the national intelligence system (article 2). This approach leaves the membership door open to the Ministry

of Justice's Department of National Prisons. In Decree 3695 (December 2000), the Brazilian government created the Public Security Intelligence Subsystem, encompassing the Ministries of Justice, Treasury, Defense, and National Integration, together with the Institutional Security Cabinet of the president of the republic. The Intelligence Subsystem reports to the National Secretariat of Public Security of the Ministry of Justice. The executive organization for the subsystem is its Special Council, whose members are the national secretary of public security (presiding); one representative from the intelligence organization of the Federal Police and one from the Highway Police; two representatives from the Treasury Ministry; two from the Defense Ministry; one from the Institutional Security Cabinet of the President; one from Civil Defense; and one from ABIN. The Department of Prisons has no representative on the Special Council.

Peru's director general of intelligence in the Ministry of the Interior (DIGIMIN) coordinates and centralizes intelligence related to internal order, public security, organized crime, and new, transnational threats. Although Peru's intelligence law (2005) does specify that political, economic, and social issues are the province of the non-military elements of the system, it labels neither the Ministry of Justice nor the National Prison Institute as parts of the national intelligence system.

The 1996 Guatemalan Peace Accords restricted army intelligence to activities in the defense environment. A 2005 law made the director general of civilian intelligence (DIGICI) responsible to protect against organized crime and common crimes. DIGICI also protects the political, economic, social, industrial, commercial, technological, and strategic interests of the country; that is, its area of concern lies in internal environments, criminal intelligence among them. The DIGICI, together with the National Civilian Police and the director-general of prison centers, reports to the minister of government, an arrangement that would lead one to expect some level of coordination among these organizations. However, despite the DIGICI's charge "to gather and centralize information coming from the organizations subordinate to the Ministry of Government," coordination remains minimal because no document yet defines the roles and responsibilities of each of these organizations.

Ecuadorian president Rafael Correa declared in 2009 that the National Intelligence System (SNI) will operate under a new National Intelligence Plan.[598]

Ministerial Accord number 26 states that the Secretariat of Intelligence, as the lead organization of the national system, plans, guides, and coordinates intelligence collection, processing, and production. The SNI encompasses military intelligence for national defense, police intelligence for internal protection, and the president's Internal Security Management Unit. The accord also notes that "other intelligence agencies that may be created or added in the future" will participate in the SNI, along with "other institutions and agencies that have or produce information of interest to the overall security of the state." In brief, the decree ignores prison intelligence, although it leaves open the possibility that new agencies may emerge and become part of the SNI. For now, the SNI includes only military and police intelligence, with coordination accomplished by the Secretariat of Intelligence.

Colombia's statutory Law Number 1621 (2013) presents definitions, limits, purposes, functions, and principles that regulate intelligence and counterintelligence activity. The law posits an "intelligence community" with a civilian organization to coordinate its work. A Joint Intelligence Council (JIC) reviews issues related to the security and defense of the state. It also coordinates intelligence and counterintelligence and ensures cooperation among the different agencies that carry out those functions. Members of the JIC include the Ministry of National Defense, the chief adviser on national security, the national vice-minister for national defense, the chief of joint intelligence (representing the commanding general of the armed forces), the chiefs of intelligence of the army, navy, and air force, the director of police intelligence, the director of the Financial Information and Analysis Unit, and the "director of any other intelligence or counterintelligence organization brought into being by law to carry out these activities." The 2013 law also specifies that public and private entities can cooperate with intelligence and counterintelligence organizations, and that if the information requested is legally protected from release, the intelligence organizations and private or public entities can create mutual agreements to accomplish the exchange of information. In short, even this detailed approach ignores the intelligence role of the Colombian prison system, although the rationale for its inclusion seems clear.

Nicaragua has neither an intelligence law nor an intelligence system. The National Civilian Police and the National Prison System both report to the Ministry of Government, but no formal arrangements exist for these

institutions to engage in coordination. The National Civilian Police has an intelligence unit among its "national specializations." This unit reports directly to the Defense Information Directorate.

Costa Rica offers another example of a country without an intelligence law. Here, the law that regulates police forces (enacted in 1994) addresses intelligence incidentally by establishing the Directorate of Intelligence and National Security (DIS) as the national security information organization serving the president of the republic exclusively. However, the DIS does not appear in the organizational diagram of the police; instead a Department of Police Intelligence appears under the Operations Directorate of the police. Because Costa Rica does not have armed forces per se, the intelligence entities under the police umbrella are the only intelligence agencies in the country. The 1994 law does not prescribe where or how intelligence can or should act, instead only stating that it is to "detect, investigate, analyze, and communicate to the President of the Republic or to the Minister of the President, information needed to prevent developments that may imply risks to the independence of the country or its territorial integrity, or put in danger the stability of the country and its institutions."[599] In the wake of a scandal over the use of sensitive information by DIS for extortion purposes in February 2011, the Costa Rican congress debated whether to revoke the authority of this directorate.

In Honduras, Legislative Decree 211-2012 (2013), created the National Directorate for Research and Intelligence (DNIE) as an independent, nominally civilian organization responsible to the National Security and Defense Council. The decree established an intelligence system, but prison intelligence has not yet become a part of it.

Bolivian political leaders see a need for an intelligence law. A proposed bill calls for greater centralization and control over intelligence activity through the creation of a Directorate of Intelligence for the Plurinational State (DIDEP). Beyond the intelligence work carried out by military and police authorities, DIDEP envisions bringing the capabilities of five executive branch entities together to create strategic intelligence: the Ministries of International Relations, Economy, Autonomy, Development Planning and the Fight Against Corruption. The legislation also seeks to address "internal control" of intelligence activities through the Plurinational Assembly, and to carry out external control through the Supreme Defense Council. Once

again, the proposed legislation makes no mention of potential information and intelligence collaboration between the Bolivian prison system and the DIDEP community. [600]

In Uruguay, after numerous congressional debates about how to establish an institution for coordinating state intelligence, and after the executive branch itself proposed a bill in congress to establish an intelligence law,[601] in November 2011 both chambers of Congress approved a special commission to write a national intelligence law.[602]

Uruguay and Costa Rica have ongoing legislative debate about institutional arrangements for the intelligence services. This development marks a positive response to intelligence-based scandals or at least improper use of intelligence information. Congressional debates about intelligence in a democracy constitute an opportunity to improve mechanisms for the coordination and control of intelligence activity. Even so, access to intelligence information typically remains "limited to those who directly control the system. The general public is excluded, along with academia, and often, even elected representatives of the people do not have access."[603] For this reason, but also because strategic intelligence often involves public policy formulation, intelligence can and should be discussed in public forums.[604] This does not mean that intelligence information itself needs to be made public. Congressional and public debates instead address what institutions and what areas of national life appear suitable for intelligence activities, potentially including areas beyond the traditional military and police environments.

Preconditions for the Emergence of Prison Intelligence

There are several reasons why it seems desirable to include national prison systems in the circle of organizations that carry out intelligence activities. In practice, though, few Latin American countries leave open—even indirectly—the possibility of collaboration between prison intelligence and a national intelligence system. Countries where collaboration appears possible include Argentina, Brazil, Chile, Colombia, Ecuador, and Guatemala. Although national laws increasingly address intelligence activity, the conceptual challenge of including prison system perspectives in intelligence systems remains unmet. Existing studies depict the unseemly nature of the prison environment in Latin America.[605] Leaving aside any indecorous comments

about that environment, the present essay will now explore three deficiencies that impede the integration of the intelligence function into the prison environment, and the flow of information from that environment into the national intelligence system:

a) **Deficiencies in prison infrastructure:** Inmate crowding exists alongside deteriorating physical facilities. "Prisoner stacking" breeds poor sanitary conditions, high levels of violence and too little spatial segregation of inmates according to the nature of their crimes. These conditions make security and control difficult for prison personnel. Further, the conditions facilitate the spread of criminal behavior, including the commission of crimes inside the facility. Intelligence collection becomes difficult but increasingly needed, given the overwhelming disorder that generates continuous tension. Riots, fires, hangings, and other violent acts can break out at any time. It is an environment where prison guards have to negotiate with prisoners to maintain some degree of order. Informal agreements spur disrespect, putting everyone's security at risk. Even under such deplorable conditions, an information and intelligence mechanism can channel information to local decisionmakers so that prison managers can prevent the worst outcomes.

b) **Insufficient professional preparation:** To maintain a dialog with counterparts in military, strategic, and police intelligence, prison officials need improved professional training and education. Often, their training is too brief—a matter of months; in other cases, prison officials are former police officers who, following a brief orientation to the prison environment, are placed on the job; in still other cases, personnel receive no training whatsoever. A truly professional preparation for prison personnel would familiarize them with principles of public security, criminology, intelligence, strategy, law, and public administration, among other subjects. Although the breadth of this preparation may seem excessive, it would increase the likelihood of an appropriate

integration of this specialty with the larger security system of the country.

c) **Insufficient security controls:** On top of the control problems that accompany prison crowding, a wholesale lack of appropriate technology makes it difficult to address the problem. Equipment to block mobile telephone signals, metal detectors, and drug detectors would bring a reduction of crimes committed from within the facility. They would also improve visitor monitoring.

It may be that Latin America has favored an over-centralized approach to prison administration. Too much centralization may impede a process of periodic, subregional or provincial experimentation that tests the value of applying intelligence in this environment. The Latin American approach appears quite different from that typical in the United States, where prison officials can choose not only to apply intelligence practices within their facility, but also to collaborate or exchange information with intelligence organizations across the country. The Regional Information Sharing System Program (RISS) and the Joint Intelligence Sharing Initiative between the Federal Bureau of Investigation and the Federal Bureau of Prisons help prevent violence and safeguard public and institutional security.[606]

Institutional modernization can begin with a review and update of regulations, laws, and decrees surrounding the mission and functions of prison administration, with an eye to creating a security system that involves collaboration among a variety of institutions. Any new regulations should consider establishing professional schools for those whose responsibilities involve prison security and overall prison operation.

Modernization should build a clear distinction between personnel responsible for prison security and those charged with the reinsertion of inmates into society. This approach would help ensure a better allocation of budgetary resources, since funds tend to flow toward the security function at the expense of social reinsertion programs. An intelligence unit or department would best be housed in the offices dedicated to security and control of each prison, to promote continuing collaboration with police and other judicial branch entities.

With a clear approach to prison management, improved physical facilities, an adequate level of security, and a more professional staff, one should expect greater integration of prison management with a national security system. National stakeholders would come to consider prison intelligence an indispensable addition to existing police capabilities. However, coordination needs proactive participants, as it occurs only sporadically and in response to specific requests from national police or military intelligence organizations. Further, prison system personnel need adequate professional preparation to earn the respect of national security system representatives. Otherwise, any coordination that does occur will not likely produce the desired results, and the incarceration system will not attain the important position it warrants in a modern, collaborative, security system.

Conclusion

Returning to the questions posed in the introductory paragraphs, the essay showed that prison system institutions can create the strategic intelligence needed to position themselves, through information and intelligence sharing, as key participants in maintaining long-term security and an informed administration of justice. Intelligence operations carried out in the prison environment can detect new types of criminal activity and discover how they may be orchestrated. A strategic use of intelligence will allow for an improvement in the administration of prison facilities and will generate additional interaction with external institutions such as the police and the judicial system as a whole.

In strategic terms, the integration of prison systems with other elements of a national security system through shared intelligence perspectives will bring a greater capability to achieve overall national security objectives. If one considers that a security strategy consists of aligning ends, ways, and means in collaborative fashion toward accomplishing a particular goal, then prison intelligence has value insofar as it provides the means to promote collaboration and bring more and better information to bear on the ultimate goal of public security. This strategic vision of prison intelligence will allow administrators to escape a more traditional outlook in two ways: prison administrators will no longer consider information from inside their facility as being relevant only to them, and other elements of the national security system (armed

forces, police, and the judicial system generally) will begin to see prisons as equal, valid, and legitimate counterparts in their daily work.

Effective intelligence management can bring positive change to inhuman and hardly secure conditions in a country's prison system. Meeting that goal depends on having personnel trained in the production of intelligence information, and having in place better prepared and well informed prison guards and administrators. For all this to come about, those in charge of managing a country's prison system, as well as the managers of its security and defense systems, need to see prison security and national intelligence personnel as peer partners. They also need to develop common mechanisms for understanding each other by communicating through intelligence sharing, thereby improving overall risk management.

From the overview of intelligence laws in this essay, one can see that the countries of Latin America (Central and South America) are far from bringing prison intelligence into the fold of national intelligence systems. Even the newer laws that reflect the modern face of intelligence have not moved in this direction. Instead, they preserve traditional military and police visions of intelligence, although they tend to leave open the possibility of accepting other organizations into national intelligence communities at a secondary level. In view of high levels of public insecurity and complex manifestations of organized crime, legal institutions require improvements in management and overall professionalism. Both tactical and strategic intelligence need attention. Information for short-term use in criminal investigation and intelligence operations needs to accompany assessments useful for long-term planning and for identifying systematic problems. The full range of intelligence capabilities will facilitate the management of security resources in prisons as well as in the world beyond prisons.

Author's Biography

Liza Zuniga Collado holds a master's degree in political science, with emphasis in international relations, from the *Pontificia Universidad Católica of Chile*.
Email: *llzuniga@uc.cl.*

Intelligence Autonomy, Accountability, and Internal Security: Foundations for Oversight

Russell G. Swenson
and
Zulia Yanzadig Orozco Reynoso

"O would some Power the small gift give us to
see ourselves as others see us!"
–Robert Burns, "To a Louse," verse 8.

The kinship felt everywhere among intelligence officers promotes international information sharing. However, the same clannish sentiment can contribute to an unprofessional worldview. Luckily, practitioners can develop greater professionalism by reflecting on their own societal role through the insights of astute observers from outside the intelligence fraternity.

The *Texas International Law Journal* offers one outsider's insights on intelligence sharing practices in a way that affirms the wisdom of Robert Burns's poetic line.[607] Any practitioner will recognize that direct exposure to a foreign culture allows one to see familiar turf from a fresh and newly appreciative perspective. Learning a foreign language builds an understanding and appreciation of the nuances of our own language. If professionalism means knowing enough about the institutional, social, and cultural environment in which one works to be aware of when one is promoting the society's well-being and abiding by the principles embedded in the United Nations' Universal Declaration of Human Rights, then these truisms apply to the authors' reading of Elizabeth Sepper's law journal article.

Sepper recognizes that extensive international intelligence-sharing networks can govern themselves, but they remain insufficiently accountable for their actions. She notes that intelligence sharing among nearly all the world's intelligence services depends on personal, informal relationships rather than the formal authority of enduring, legal frameworks. This approach reduces the viability of internal accountability and external oversight as intelligence autonomy circumvents democratic safeguards established by domestic law and international treaties. Sepper explains how intelligence sharing within

the framework of international law might become more accountable to governments and international legal norms.

The following review essay derives from the authors' reflection on Sepper's work and their own familiarity with the U.S. and Mexican intelligence systems.

Environment of International Intelligence Information Sharing

Several factors have combined to propel the development of extensive bilateral relationships and occasionally multilateral networks dedicated to sharing information between intelligence services. Informal relationships for intelligence sharing exist even among ideologically disparate countries. The U.S. Central Intelligence Agency maintains over 400 information-sharing arrangements with foreign intelligence organizations (an average of more than two per country), and Britain has 120 such ties.[608] The urgent needs of World War II promoted the phenomenon, with the Office of Strategic Services, precursor to the CIA, as ringleader.

The post-Cold War intelligence environment brought other factors into play. Information technology allows illicit organizations to develop quickly, increases their ability to take action, and allows them to remain highly mobile. The licit world applies the same technology to gather clues about the location and nature of illicit activity.[609] International intelligence sharing responds to the worldwide demand for those clues. The idea that national services are not equally effective in all spheres of the intelligence function creates another basis for the international exchange of intelligence information. Deficiencies in human-source intelligence (HUMINT), for example, undermine U.S. proficiency in technical intelligence collection capabilities.[610] Such disparities encourage one country to share information from a potent intelligence collection discipline with another state whose data collection expertise lies in other areas.

Where intelligence information exchange between two prospective partners does not stem from an historical relationship, useful data exchanges may depend on another rationale. The economic concept of "relational contracting" explains why neither side in a prospective trading relationship has sufficient incentive to renege on a contract or to deceive the other. In a hierarchical intelligence relationship, where a more powerful state exerts some oversight

over the intelligence activities of another state, relational contracting reduces the likelihood that shared information will be deliberately incorrect or inaccurate.[611] The relationship between U.S. and Colombian intelligence services in counterdrug and counterinsurgency operations illustrates the principle.

Within formal networks like NATO (for military intelligence) or the signal intelligence agencies of the English-speaking United Kingdom, United States, Canada, and Australia/New Zealand (UKUSA), intelligence sharing takes place under the auspices of specialized government agencies rather than under the eye of foreign-policy institutions like the U.S. Department of State or a foreign ministry. Independent decisions by intelligence officials to initiate or break off information sharing are not subject to public or democratic oversight. In the U.S. Intelligence Community, the president approves covert (deniable) intelligence actions and must report them promptly to the select committees on intelligence.[612] Sepper worries that no similar requirement applies to other intelligence management decisions or activity.

Although it may be possible for governments to exert controlling pressure over their own civilian intelligence services through relational contracting, the general absence of an extraterritorial application of laws means that the international environment remains essentially lawless.[613] On this stage, human rights can be violated with relative impunity, especially through secretive and deniable actions of intelligence organizations.

The scrutiny applied to U.S. intelligence has brought to light a type of human rights violation in the international environment that may occur routinely. A long-time scholarly observer of the Intelligence Community notes that in his presence, reminiscing intelligence officials recalled occasions in unidentified countries where the Central Intelligence Agency had "recruited local police chiefs to jail local citizens on trumped-up local charges until the citizens would 'sing' to CIA officers about what mattered to the agency (but did not matter so much to the local police chiefs)."[614] This example fits within the context of international intelligence collaboration and sharing, although it is not an example of information sharing. It does exemplify the unconstrained environment of international intelligence operations.

Sepper's concern that intelligence services bring unwanted notoriety to their respective states through ill-considered actions prompts her to suggest that

the legal establishment has a substantial stake as a societal arbiter of intelligence practices.

The Legal Establishment as Arbiter of Professional Practice in Intelligence

Legal scholars examine the nearly infinite variety of citizen interactions. They explore the rules governing those interactions and the relationship of existing laws to societal norms. Sepper explores the extranational behavior of public officials whose actions as employees of intelligence agencies seem beyond the reach of national legal systems. Whereas intelligence practitioners maintain that professional ethics can guide their actions even in the international environment, Sepper sees ethics as an insufficient substitute for laws—formal laws would better reflect the long-term interests of society.

Sepper distrusts international intelligence and information-sharing relationships that rely on ethical decisions to achieve congruence with societal norms. A penchant for independence among intelligence practitioners coincides with a lack of transparency. The lack of transparency in turn stems from a chain of decisions that favors secrecy. The chain begins with special protection of shared information, a step taken at the insistence of the originating intelligence service. If shared information becomes widely or publicly known, it may be traced to the original sources. Recipients of shared information cannot be trusted if they allow collection methods or the identity of individual informants to be inferred.

Special protection is afforded shared information to promote the level of trust needed for future exchanges. To be trusted by other intelligence services is the *sine qua non* underlying future exchanges of useful information. Sepper documents the reasons for her distrust of international information sharing by showing how intelligence services can capitalize on nondisclosure agreements to evade legal constraints protecting a country's own citizens from being the target of communications intercepts. One example of the misuse of a partner's trust is when U.S. intelligence services allegedly watched domestic Norwegian targets, whom the Norwegian police were prohibited from observing.[615]

A tendency for intelligence services to become less transparent as they extend their autonomy defies democratic expectations or norms. Even the

discovery of historical actions undertaken by a country's intelligence services, made possible through formal declassification procedures, becomes more difficult if foreign information was involved.[616] Sepper notes that a hesitancy by practitioners to expose intelligence sources and methods to discovery through the court system hinders the ability of public media to monitor government actions.[617] Intelligence services have an incentive not to share information from abroad even with sister agencies in their own country. This practice increases the vulnerability of a country's population to the actions of dangerous international groups. In the U.S., retrospective investigation into the information environment prior to the 9/11 attacks reveals several instances where such information was held too closely within the externally oriented agencies of the Intelligence Community, contributing to the success of the terrorist attacks.[618]

Legal scholars approach the application of societal norms to the international environment from the embryonic baseline of international law. International law has benefited from the creation of international conventions, to which most countries voluntarily adhere.[619] However, a general lack of enforcement mechanisms tied to these conventions means that the threshold for accountability among government agencies remains unmet.[620] This lack of enforceable accountability, except in cases where two states agree to international jurisdiction to resolve disputes, means that under international law, just as for intelligence agencies operating in the international environment, peer pressure is the chief recourse to signal appropriate behavior among peers. Supranational laws or agreements cannot yet enforce restraints on intelligence actions.

Legal scholars like Sepper seek to bring intelligence agencies and their international sharing agreements and activities into the circle of behaviors sanctioned by societal norms. However, the continuing lack of enforceable accountability for even the existing international conventions argues for a different approach to restraining intelligence activities. The variety of non-democratic behaviors exhibited in international intelligence-sharing practices calls for a serious exploration of alternative strategies to achieve democratic accountability and oversight of intelligence practices in internal as well as international environments.

Maintaining a Tradition of Decisionmaking Autonomy within Intelligence Services

Tennis players know the value of participants themselves making out-of-bounds calls in a non-refereed game. Even though the opponent makes the in or out call, both players recognize that the player closest to the location of the ball has the best opportunity to make the correct decision. Furthermore, each player recognizes a good reason not to cheat—building a reputation for personal integrity in the tight circle of good players. Similarly in the national intelligence services, with the credibility of a source or the validity of information on the line, the agent in the field or the all-source analyst managing a desk, and not the president's national security adviser or a congressional oversight committee, becomes accountable for evaluating a decisive intelligence input. Additionally, for tennis players as well as intelligence practitioners, rarely are individual decisions made without the on-looking, interested eyes of at least a few spectators or colleagues. An ethical outlook toward professional accountability grows from awareness of and participation in collegial and conditional legitimization of one's actions and decisions. The evolution of this awareness has contributed to the invention of a new, English-language, international journal on intelligence ethics.[621]

The recognition and observance of professional ethics support the continuation of substantial autonomy of decisionmaking in the intelligence services, to include the realm of international information-sharing practices singled out by Sepper as ripe for a more formal and broadly based accountability. By definition, intelligence services occupy and act in the niche between the information needs of a society's political leaders and difficult-to-obtain, incomplete sources in both domestic and international territory. In this politically charged and uncertain information milieu, intelligence decisionmaking autonomy forms the backbone of independent, objective assessments that in turn support the independent operation of an agency.

The existing tradition of decisionmaking autonomy in intelligence services originated in the military environment. In relatively compartmented and hierarchical military organizations, intelligence is designed and expected to take the lead ahead of logistics, operations, and even planning, especially in preparing for strategic decisions. A camaraderie develops among practitioners of

military intelligence who share secrets denied even to their operational brethren. The clubbishness augments their autonomy, as they set themselves apart from the "unwashed" who are not privy to secrets, nor to the sources and methods that generate the secret knowledge. The exclusivity and separateness derived from military intelligence, as it contributes to a sense of exclusivity, extends to foreign liaison arrangements where national (largely civilian) agencies such as the U.S. National Security Agency (NSA) operate with extensive professional autonomy.[622]

Sepper contends that a process of acculturation, rather than the threat of punitive sanctions, explains why intelligence agencies in developing countries tend to conform to the standards of behavior professed by leading international intelligence services. Various authors whose work she reviews explain that "shaming" and "shunning" among the members of a relatively small and cohesive group like the intelligence fraternity bring effective negative pressure. Positive incentives include "displays of public approval."[623] Sepper contends that the United States and the United Kingdom, in particular, have acculturated their partners to relatively arbitrary standards of behavior."[624] The UK appears highly sensitive to foreign disapproval of the professional competency of their intelligence services, evidenced by the effort to prevent publication of a retired assistant director's exposé of illegal and incompetent actions within the UK's civilian, internally focused MI5.[625]

Politically powerful states like the U.S., through the actions and reputation of their intelligence agencies, can acculturate existing partners and aspiring partners (with or without financial and training incentives) toward the use of the polygraph to vet practitioners, toward the acceptance of "counterterrorism" as a catchall term for criminal and some ideologically oriented political activity, and finally, toward the favored development and employment of national security agencies (military intelligence as well as internationally oriented, civilian intelligence agencies) rather than domestic or even international police institutions.[626] Thus, it is not external "control" exerted by judicial, legislative, or executive powers that brings intelligence decisionmaking into compliance with an international norm, but rather a social process of acculturation to the standards espoused by leading, powerful states.

One caveat to internal accountability among intelligence services needs to be acknowledged: Accountability among national security intelligence services

exists as a series of immediate decisions, and not as a long-term or necessarily consistent process. The achievement of greater consistency requires greater concern for long-term trends embodied in political ideas and ideals with worldwide reach. Foreign intelligence services tend not to represent the ideals of their respective countries because civilian agencies in particular are relatively new institutions, dating only to World War II, and in their current state, only to the end of the Cold War. The sense of immediacy that surrounds intelligence service accountability stems from a necessary focus on the actionable future rather than across the sweep of history, making them more or less isolated from the mainstream base of ethics and accountability where laws embodying the evolutionary *zeitgeist* of the society have been developed and applied based on popular will and political process. Therefore, out of concern that national security intelligence personnel and institutions be more thoroughly accountable and subject to legalistic oversight, this essay will now explore a universal and nationwide security institution with decisionmaking autonomy in information collection for intelligence purposes. This instititution also embodies the behavioral and attitudinal norms of a broad spectrum of its respective society.

The Police Intelligence Model for Professional Accountability and Oversight

The ascendance of the "public security" concept to replace "national security," the increasing popularity of community-based policing, and the advent of intelligence-led policing in various parts of the world all signal a greater integration of local with national interest in personal safety and civic responsibility.[627] Michael Herman, a leading observer of international intelligence issues, asserts that "[w]hile only one state (or coalition of states) can win a war, trade contract, or border dispute, most states benefit from reduced drug trafficking or terrorism—it is not a zero-sum game."[628] Could the same insight apply to the scene inside one country? For this observation to hold true for any particular country alone, it must exhibit an equal application of measures to improve public security across the national territory. Otherwise, given the mobility of sophisticated criminal organizations, criminal activity endangering public security can erupt where it is not actively suppressed. As immortalized by the "Western" television and movie genre, bringing "law and order" to the frontier depended on local community demand for a dependable

sheriff, backed by regionally deployed federal marshals. This model makes community-based and intelligence-led police the new and essential "lawmen" on the information frontier where tensions between criminal activity and public security demand resolution. Organized criminal entities will also have discovered the synergy of intelligence-led planning and community-based recruitment in their own operations.

Sepper alleges that if intelligence practitioners were to allow their practices to be scrutinized by the justice system in their respective countries, then "[a]rrest and prosecution of suspects, instead of detention and torture … would check abuses and engender public support." She further recommends "[t]reating terrorist violence as a criminal act—to be handled through legal systems in accordance with the law, democracy and human rights."[629] With the terrorism label, the U.S. intelligence system has acculturated itself and partners toward keeping domestic counterterrorism and worldwide actions against ideologically motivated behavior outside of the legal system where police, prosecutors, and judges operate.[630] Intelligence officials fear the exposure of sources and methods during court proceedings. Sepper contends, however, that "courts are adept at finding creative solutions to protect information while allowing for an effective defense."[631] She adds that "[t]he involvement of courts has several distinct advantages. It advances Western intelligence's interest in accuracy and the pursuit of truth, which facilitates the protection of democratic states, a task at the heart of these agency's missions."[632]

One result of the tendency to keep national security intelligence separate from police circles and legal systems is that police agencies have had to develop informal, international networks of information exchange that rely on the individual willingness and ability of government officials to share sensitive information without the benefit of formal approval by senior officials.[633] Because of its informal and off-the-record nature, this approach can result in continued underfunding of law enforcement activity compared to the resources lavished on national security/intelligence institutions that accept and act within the framework of "counterterrorism."

The counterterrorism approach to illicit or outlandish behavior gains public support when reviled, key figures are killed or captured. Additionally, comparative underfunding of law enforcement detracts from Sepper's recommendation to employ intelligence-led police agencies and the criminal justice

system against all targets, whether ideologically motivated or not.[634] Because Sepper's approach would nonetheless support the twin aspects of accountability: 1) transparency and 2) being subject to negative or positive sanctions, a disconnect or contradiction (not merely tension) exists between too few resources being obligated to satisfy the society's normative priority for public security through its legislative and judicial framework, and the abundance of resources available to the national intelligence services, which lack accountability.

Figure 9. Mexican Navy Team
Source: Photo by Zulia Orozco.

As an exercise in reducing this discontinuity, a new law in the Mexican state of Nuevo Leon represents a rare subnational initiative that should assist the criminal justice effort against narcotrafficking groups who employ *halcones* (lookouts) to spy on police movements.[635] The new state law for the first time establishes criminal penalties for those who serve as lookouts during operations staged by narco-traffickers in the state. This legal resource will back up any effort by police intelligence operatives to identify and question

at least those who engage in this form of local collaboration with criminal groups. The threat of imprisonment may encourage the identified lookouts to provide further information about criminal activity. At present, this initiative is limited to one state in Mexico, but if successfully implemented it could signal a turnaround in the tendency for new resources to be directly mainly to national-level public security forces.

At this juncture, one may ask whether intelligence-led police agencies observe internal accountability precepts in their decisionmaking. Because police institutions are thoroughly embedded in the justice system of a country, and because their collection of evidence must pass the threshold of open, oral, and adversarial court procedures, this route to information use does offer the transparency that defines an important aspect of accountability. To satisfy the second aspect of accountability, positive or negative sanctions must come into play. The U.S. cultural affinity for the use of the counterintelligence polygraph constitutes a negative sanction for the personnel of U.S. military and civilian intelligence agencies, and it is being passed on to intelligence partners. In Mexico, for example, polygraph has been employed as a "confidence test" administered even to veteran police employees.[636] Its use may extend to ensuring that human rights are not violated by officers of the law in the course of collecting and using intelligence information. Intelligence-led policing can thus address both aspects of accountability.

Figure 10. Members of the Mexican "Zorros"—Special Police
Source: Photo by Zulia Orozco.

Community-oriented, paramilitary police agencies that employ disproportionate violence are subject to the criticism of adopting an aggressive military-style ethos. The militarization of police agencies has a potential counterpart on the national and international level: the policialization of the military. Policialization may be thought of as a tendency for the military to reduce the use of overt force. An example of this approach from an intelligence perspective comes from intelligence-led U.S. operations in Iraq and elsewhere.[637] In the words of one participant, operatives of the Joint Special Operations Command have begun to use less coercive interrogation methods to gain information from low-level detainees, who are then released if their information proves useful and accurate.

If a central purpose among internally deployed military personnel is to exercise their intelligence capabilities by developing informants as they build community relationships, then the potential for the military to adopt a less forceful approach becomes feasible. A military led by intelligence to sharpen the blunt instrument of national security forces should not be an unexpected development, given the tradition of intelligence being the acknowledged lead element among the specialized military functions. This scenario could become a model for local police integration with national intelligence capabilities mediated by military or national, civilian institutions.[638]

The Mexican Federal Police plays a preventive intelligence role across the country.[639] It has all the necessary resources to develop its own investigations. Research undertaken by the authors reveals that the most advanced state police in Mexico (in the state of Queretaro) maintain database information that allows them to generate preventive intelligence. That information allows police organizations to compare crime data and take proactive steps; however, most state institutions responsible for public safety (such as the states of Yucatan or Zacatecas) have deficiencies of trained staff, and the agents fear exercising their institutional role because the Mexican government cannot ensure their long-term security against organized crime.[640]

Recent developments in Mexico offer a case study of how local police information gathering has been usurped by military forces. In several localities in Mexico, military forces have uprooted local police establishments. An interview by one of the authors with a local police official who worked in a municipality where the military has taken control of security, reveals some of the dynamics accompanying the contest between local and national security and intelligence institutions. The police official said that despite their having the technological equipment necessary to inform the federal government of criminal activity through the *Plataforma Mexico* (the principal database on organized crime), administrative authorities of the municipality expressly forbade adding comments or uploading information about serious situations such as shootings or kidnappings to the platform. The rationale for this approach was based on fear.

According to the interview subject, police administrative authorities feared two scenarios, the first of which became a fact:

1. Fear that the federal government would send more troops to the area, and / or

2. Fear that the federal government would not send financial resources for public security programs such as the Public Security Assistance Fund (FASP) and Subsidies for Public Security in Municipalities (Subsemun).

However, after personal reflection on the potential consequences and administrative reprimands that could result from such negligent actions,

the administrative staff changed their mind and decided to allow entering information about all situations into the database. The interview subject confirmed that given the violent situation, military personnel took complete control of local police facilities in 2011. According to the agent, police officers were relieved of duty without argument, and are now in line to be trained under a certification program, even as the military remained responsible for the safety of the location.

From a citizen's perspective, public safety in Mexico has deteriorated. In reality, this is a matter of perception, as the data show a variable picture. According to the Citizen's Institute for the Study of Insecurity, public trust in the police force, compared to trust of the army, is relatively low.[641] Survey results speak of distrust and even a broken police/community relationship, evidently because of the opacity, corruption, inefficiency, and ineffectiveness of police work that includes the hazardous specialty of police intelligence.

Figure 11. Mexican Federal Police Team
Source: Photo by Zulia Orozco.

A condition for police intelligence to succeed as part of an authentic, community-oriented security agency, assuming the existence of budgetary parity with national security institutions, will be the society's evolution toward independent, adversarial courts and successful prosecutions. The best intelligence information comes from participants who inform government authorities of future criminal actions; therefore, developing witness-protection-style programs for whole families would show prospective informers that informing is not a death sentence. Especially in a society where extended families can be targeted for reprisal, protecting the identity of undercover informants is central to the prosecution process. In the absence of human intelligence assets being able to penetrate the closed circles of native criminals,[642] the best available alternative is "technical intelligence"—the proved capability of communications interception to provide relatively unimpeachable court evidence. The product of technical intelligence does not reveal the identity of the collector, even if some details that lead to effective collection by this means were to be provided by "insider" informants. Those individuals can remain unknown and unidentified in court. A likely scenario would be for an informant to emerge in the aggrieved locality, and for the technology for collecting and processing communications intelligence to be a state or national resource. In this scenario, the ethos of the community and the resources funded by representative government come together to distill the individual and collective preferences of the citizenry, thereby bringing to life the ethical ideal of having intelligence activity tied to the society's values.

Discovering a Preferred Model for Democratically Flavored Accountability and Oversight for Intelligence

As spelled out by legal scholar Elizabeth Sepper, the outsized autonomy of international intelligence-sharing practices calls for redress to protect democratic ideals. The present authors' review of her work from a government intelligence perspective moves from an examination of the validity of her argument that the legal system can wisely arbitrate a reduction in the autonomy of intelligence services, to an evaluation of alternative approaches to achieving a suitable level of intelligence oversight and accountability. Intelligence oversight exists within a legal framework designed and implemented by legislative and judicial branches in a functioning democracy. Accountability involves openness on the part of professional intelligence agencies to inspections of

their practices and the application of negative and positive sanctions to their work, notably including the application of budgetary priorities.

The desire by legal scholars to arbitrate the conduct of intelligence activity, at least on the international level, does not match the need to bring accountability to intelligence practices. This is chiefly because no dependable mechanism yet exists for exerting sanctions against international intelligence sharing practices. Intelligence-led police agencies can achieve authentic accountability, and because they are embedded in the judicial system, they have a natural orientation to the rigors of legally oriented oversight.

A different version of this essay appeared on the Web site of the Institute for Security and Democracy (Insyde), a Mexican security studies center, at http://www.insyde.org.mx/shownews.asp?newsid=708.

Authors' Biographies

Russell G. Swenson served from 1988 as professor, and from 1995 through 2008 as director of applied research at the National Defense Intelligence College (now the National Intelligence University). He also directed the NDIC Press from its inception in 2006. He has authored or edited numerous publications on intelligence process (*http://www.ni-u.edu/ni_press/press.html*). In earlier years, he worked as intelligence analyst and linguist in the U.S. Air Force and as associate professor of geography at Western Illinois University. He holds undergraduate degrees from the University of Kansas (geography, Spanish, Latin America area studies) and from the University of Wisconsin-Milwaukee (master's and doctorate in geography). He was awarded the National Intelligence Medal of Achievement, and in retirement he continues to collaborate with officials and researchers in the field of strategic intelligence. **Email:** *drintel2@yahoo.com.*

Zulia Yanzadig Orozco Reynoso holds degrees in law and sociology from the *Universidad Nacional Autónoma de México* (UNAM). She has worked with the Mexico City-based Institute for Security and Democracy (INSYDE) on several projects, among them civil monitoring of police and security Forces in Guerrero state, the role of an independent police auditor, and the creation of an index of transparency and police accountability. In the latter project she collaborated with representatives of the 32 state police organizations of

Mexico. Zulia is currently a United Nations consultant on citizen security in Latin America and a doctoral student at UNAM. **Email:** *zulia.orozco.pnud@gmail.com.*

Section Four
Managing Intelligence Integration: A Challenge for Intelligence Services

Intelligence Education and Integration: A Symbiotic Relationship

Anne Daugherty Miles

Intelligence agencies face the continuous challenge of integrating their efforts to become a more capable community. For example, a real or perceived "wall" inhibits the exchange of information and assessments between the world of police intelligence and national security intelligence. Additionally, functional and geographic separation can lead to or exacerbate differences in organizational culture and/or technology that impede the desire to collaborate. Sometimes these obstacles can be partly overcome with legislation. In the 1980s, for example, the U.S. Congress addressed the critical need to integrate service-specific cultures by passing legislation known as the "Goldwater-Nichols Act,"[643] which mandated and rewarded "jointness" and required "joint professional military education." The clear link between education and jointness transformed and integrated the existing system of professional military education.

Jose Paz's essay, "The Education of a Strategic Intelligence Professional: Fulfilling National Expectations," focuses specifically on the link between education, integration and innovation. He suggests that a joint or holistic approach to intelligence education brings about the integration and innovative thinking needed to address pressing problems such as cybersecurity. Paz argues for intelligence education that provides "deep knowledge" and is career long. In addition, he believes that academic freedom must exist "along with room for creativity, interaction and energetic inquiry." In short, he sees education as the vehicle for learning to think critically, to question assumptions, and to hone skills of abstraction and analysis. The educational requirements and opportunities he envisions could help to increase public trust as intelligence practitioners become more widely perceived as *intelligence professionals*.

Increasingly, the problems threatening citizen and national security in our respective nations need the collaboration of many disparate players in holistic, thoughtful, strategic, short-term and long-term analysis. What better place is there to hone such skills and develop a network of life-long friendships than intelligence graduate institutions—especially if they bring together players from not only the defense, intelligence, and law enforcement communities,

but also from academia and business? Paz's essay suggests that these institutions offer a perfect place for parallel public and private universes to intersect. Although many intelligence education institutions opt for classrooms closed to those without badges, Paz argues for openness. "Although secrecy is appropriate when and where prescribed by law, it cannot extend to the academic world." He would save secrecy for the training environment, and use openness in education venues to shine a light on the big problems of the day—arguing that those problems need the collective wisdom of a nation's best and brightest: "Secrecy is neither necessary nor appropriate for academic success, especially in view of the idea that today most intelligence is developed from open sources…."

As Swenson's introductory essay to this book suggests, we have come to depend on accurate and timely intelligence for "public security, civilian and military planning, and even economic well-being." So pervasive is the requirement, and so great is the threat, that the need for true integration of all sources of "intelligence"—public and private—appears immediate and imperative. That message pervades Robin Rogers's essay on cyberspace security, the second essay in this section. In his essay, "Managing Intelligence Information for Multinational Cybersecurity—Approaches by the United States and Brazil," Rogers brilliantly encapsulates the need for an integration of cyber incident information across all levels of government and all levels of public and private domains. He reminds us that cyberattacks happen daily, integration is necessary, and "the essential ingredient of this coordination is sharing information–whether proprietary information, law enforcement information, or intelligence information." Cybercrime acts as an "intermestic"[644] issue, presenting both a domestic and international security challenge, therefore involving many players in government security.

The Rogers essay builds on essays in the first three sections of this book that point out many roadblocks to sharing information. He reminds us that obstacles include uncertainty over what to share, institutional "territorialism," issues of trust, and concerns about potential abuse of civil liberties and human rights.[645] Other obstacles to information sharing are more a result of institutional separation—both geographic and functional. Rogers adds the observation that "these obstacles are compounded when countries need to share intelligence information with each other."

The other two essays in this section provide practical advice about how to overcome obstacles to information integration between countries—to include the knotty problem posed by Rogers. The Paz essay offers an education-based solution while Brei *et al*. suggest a team construct. Both solutions depend on achieving some measure of collaborative interaction, together with integrated and innovative thinking.

Harnessing Security Sector Intellectual Capital: Transforming Advisor Situational Awareness into Sociopolitical Understanding in a Smart Power Environment, by Brei, Frensley and Roberts (three veterans of the International Security Assistance Force campaign in Afghanistan) demonstrates how an advisory mission to promote the development of national-level governmental institutions requires an innovative information development and handling philosophy to deal effectively with host-nation counterparts. They explain how the team construct they created overcame the limiting legal and organizational strictures normally associated with formal intelligence operations. Their ability to transform the outlook of the advisor corps from "situational awareness" to an Afghan-centered social-political understanding depended on blending the depth and breadth of pertinent information from *both* U.S. and Afghan Ministries of Government. They would agree with Paz's desire for openness and they write about the ways in which they encouraged and maintained relationships built on *trust*. They believe that the team construct they created "captures the insights generated by its different components at the operating level and forges those insights into shared corporate knowledge across the organization."

Brei *et al.* argue that "all security sector advising missions are smart power initiatives." By that they mean that the advisory mission they supported was a "soft power" piece of a larger "smart power" strategy that included elements of both "hard power" (associated with military and economic "sticks") and "soft power" (diplomatic and humanitarian "carrots"). Investing resources in alliances, partnerships and institutions provides a critical ingredient for "soft power" as defined by Joseph Nye and others. Their essay illustrates the direct relationship between the adoption of teaming concepts and the success of soft power initiatives.

Read together, these three essays illustrate the intelligence value of education and integration. Rogers sees both as necessary ingredients to solving big

problems such as cyberspace security. Paz believes integration encourages innovation, which in turn benefits from community-wide educational institutions. And finally, Brei *et al.* describe an integration process in which the act of integrating intelligence educates *not only* its consumers *but also* its producers. Brei et al. even suggest that a major goal of intelligence integration should be the creation of "intellectual capital"—knowledge forged from the "raw intellectual material generated by individuals."

Lt Colonel (USAF, Retired) **Anne Daugherty Miles** holds a Ph.D. in American Government from Georgetown University and began service on the National Intelligence University faculty in 1995. Her specialties include resource management and the policymaking process, both taught within the framework of U.S. domestic and international politics. In 2009, Miles served as a congressional fellow on the U.S. House Armed Services Committee, and in 2010, as a legislative assistant to a member of the U.S. House of Representatives. Her award-winning essay, "Professional Intelligence Education," is available on the International Association for Intelligence Education website. Dr. Miles joined the Congressional Research Service in 2014. **Email:** *amiles@crs.loc.gov.*

The Education of a Strategic Intelligence Professional: Fulfilling National Expectations

Jose Gabriel Paz

"Dimidium facti, qui coepit, habet; sapere aude, incipe."
(He who has begun is half done. Dare to be wise; begin!)
—Horacio, "Epistularum liber primus" Epistle II

Introduction

The most significant human endeavor is the transmission of knowledge. The validity of this observation rests on the idea that the human species cannot transmit enough information genetically to provide for the social development of individuals.[646] Thus, education has become indispensable to the existence and subsistence of humankind.

Education begins in the familial environment and continues in the larger social context. It starts in the preschool years, and continues beyond "graduation," encompassing retraining, certification, and self-education. This variety of educational venues allows the individual to improve quality of life and workplace capabilities through continuous study.[647]

This lifelong aspect of education takes on considerable importance in the professional development of individuals engaged in knowledge work, where certain societal and institutional functions require substantive expertise. Education gains importance as a phenomenon when it involves the preparation of individuals for key national functions like strategic intelligence, where complex and specialized work must be done.

This essay aims to identify some of the factors that help ensure the high-quality formal education of intelligence professionals. It also offers some practical advice about how the value of that education may be measured.

Institutional Responsibility for the Education of Professional Intelligence Personnel

The professionalization of a strategic intelligence organization requires clear mission objectives and an institutional culture rooted in principles and

values. The achievement of these ideals depends on the availability of stable and specialized bureaucrats, products of a rigorous recruitment and selection process. A candidate for employment must have a university-level education and a technically adequate resumé. Of equal importance, the candidate must see the possibility of career advancement corresponding to his or her abilities, supported by the employer's objective evaluation of the employee's merits.

No longer the automatic product of an empirical or practical on-the-job learning process, professionalization grows from the ability to make knowledgeable judgments about rapidly changing circumstances. Thus, individual intelligence professionals require both technical expertise and familiarity with the highest level of postgraduate social analysis—in brief, deep knowledge.

An intelligence organization cannot avoid the requirement to undertake continuous institutional improvement and to search for high-quality prospective employees. Those candidates need to be educated in reputable institutions that refine native abilities and develop needed skills, and that instill in the individual values and habits respectful of laws and of human rights. In addition, prospective employees require an ethical conscience and skill in critical thinking, together with loyalty, a love of country, and of the profession itself.

Intelligence organizations of every country should ensure that their professional employees maintain high academic standards in their official work. Other appropriate goals: that ongoing professional teaching and learning take place within the context of the organization; that it take place in an institution of higher education (either using the organization's own educational resources of those of other educational institutions); that professional studies be carried out at the postgraduate level; and that arrangements be made for retraining or recertification through a program of continuing education.

For education to be offered at the level required, academic freedom must be combined with room for creativity, interaction, and energetic inquiry. It may appear that these traits conflict with the secrecy demanded in the professional context. Although secrecy is appropriate when and where prescribed by law, it cannot extend to the academic world. "Secrecy is neither necessary nor appropriate for academic success, especially in view of the idea that today most intelligence is developed from open sources available to everyone. Only a tiny

proportion of intelligence activity involves information obtained through special means."[648]

The concept of open education should prevail insofar as it refers to a curriculum offering a variety of topics appropriate to formal intelligence education. Open education may also refer to participation in intelligence education by those with a wide range of professional responsibilities in a given country.[649]

Openness in education holds value because

> publicly funded intelligence schools can no longer restrict themselves only to the professional preparation of their own intelligence analysts and agents or counterintelligence managers, but need to broaden their horizons by accepting and educating other public servants about the processes and culture of intelligence. Among them should be members of congress who serve on intelligence committees and, especially, their legal and technical advisors. Often, legal education and knowledge of congressional lawmaking procedures, or experience in congressional oversight, should be complemented by knowledge of intelligence and national security. The same approach should be taken with respect to judges and other officials of the judicial branch of government, especially those who authorize special operations in intelligence. Additionally, intelligence education should be extended to various other administration of justice officials.[650]

Educational Needs of Intelligence Personnel

Strategic intelligence analysts are responsible for the knowledgeable handling of a surpassing variety of topics and situations. These can include national and international politics, political and economic rivalries among states, education issues, strategy, technological advances, environmental problems, crimes, energy questions, scientific and space research, operations research, conflicts anywhere, hazardous substance handling, threats to national security, transportation issues, critical infrastructure protection, agricultural production security and more. Concepts now in technological development that will soon be used to obtain, store, and process the key information

required for decisions at the highest level also demand the attention of a strategic intelligence analyst. Analysts thus need to be superbly qualified in an academic sense.

A strategic intelligence system exists "only to serve its client or consumer, normally a president or cabinet ministers—and always a small group."[651] Therefore, an analyst's work is exceptional by virtue of providing indispensable knowledge for the decisionmaker's basic understanding, for adjusting strategy, for the adoption of measures to intervene in or influence objective realities, and for the development of information or disinformation operations for security and national defense.[652]

In practice, the intelligence analyst should

> observe the background of events, carefully review the great issues facing a country and the world, bring into play any historical phenomena that remain in play, discover trends, define new approaches to unanswered questions, pull aside the veil of deceit that accompanies simplistic answers, and outline possible futures.[653]

Technological instruments do not produce either knowledge or intelligence. Information can be gathered and manipulated with technological assistance, but knowledge creation depends on an inevitably human process.[654] In addition, no technological tool yet exists for the effective management of knowledge: Existing tools can only be understood and used in the frame of reference dictated by technical methods for knowledge management.[655] Therefore, the great value of analysts rests on their intellectual capabilities, their accumulated tacit knowledge, and their ability to manipulate helpful technical tools.[656]

In sum, only an appropriate education at the highest level and the development of technical skills allow a professional to apply scientific research methods, engage expertly in rigorous analytic thinking, and bring depth to knowledge. Additionally, the educated professional will know how to manage collection tools that will allow him or her to understand and disentangle hidden aspects of reality.

Higher Education and Educational Excellence

Selective, systematic postgraduate work prepares personnel in scientific, technological, and humanistic fields, building the type of "transcendental" knowledge needed by intelligence professionals. Higher education in South America meets the need for specialization or professional preparation by offering three categories of academic degree: a specialization (a graduate degree), the master's, and the doctorate.[657] Happily, the requirements associated with these degrees are relatively uniform across the Americas.[658] An additional specialized degree common in the region is the *Diplomado*. A candidate with credentials at that particular level of study can be evaluated on the basis of the prestige of the institution attended, the academic quality of its program of study, and the associated requirements.

The administration of academic degrees requires that one have knowledge of educational processes, direct experience in university teaching, experience in guiding a particular educational program, and knowledge of institutional management. Of course, an administrator must also hold academic degrees in a recognized discipline. It is also desirable that the administrator of an institution where intelligence professionals are prepared be familiar with the particular needs, professional profiles, and all elements, even of a technical nature, suitable for the education of a professional in the field. Additionally, all academic officials, to include administrators and faculty, as well as technical personnel, should have expertise in the field of intelligence.

The education of intelligence professionals must be guided by faculty with advanced academic degrees. The faculty also needs to be permanent and stable, so that classroom instruction and academic advice is not in the hands of "panelists" or "guest lecturers." The curriculum also needs to be systematic, and not a series of courses and seminars with no clear pedagogic and cognitive connection among them. Such inconsistencies reveal a lack of curriculum planning and a dependence on "volunteerism" characteristic of a bureaucracy unfamiliar with educational administration.

In many countries, the institutions that take on the education of intelligence professionals do not adhere to the standards for formal education prevalent in their own society. They are often not accredited, and do not offer academic

degrees that are recognized by their respective national educational systems. An educational institution that lacks mechanisms for academic control and evaluation is deficient in terms of the quality of teaching and learning. This condition also reduces the institution's ability to improve the intelligence system's articulation and integration with the real needs of the state.

When poor bureaucratic or corporative decisions impede the development of a "culture of institutional evaluation," an educational entity suffers self-perpetuating poor practices and educational staleness. The lack of an external review of the institution's purposes, efficacy, efficiency, and capabilities further degrades the quality of its services. Notwithstanding these deficiencies, a state's financial support system typically continues to operate automatically from year to year, maintaining subsidies for the traditional lineup of educational services, without linking the state's annual financial commitment to the quality, productivity, and actual results of the educational activity.[659]

Intelligence Education Structures across the Region

It might appear that the ideas expressed here about academic quality are difficult to put in practice, but several alternative paths exist to achieving educational excellence in the formation of professionals suited to the task of intelligence. In fact, some countries do make use of traditional higher-education institutions as the best alternative for the professionalization of government personnel.[660]

Countries of the region accomplish professional education in intelligence in one or more of these three modes: 1) the intelligence organization carries out its professional education using its own, autonomous academic structure; 2) the intelligence organization has its own academic institution, but some educational management takes place in external academic institutions; and 3) the intelligence organization places the entire educational process in the hands of an external academic institution. In this last case, the external institution can be either a university or an educational institution managed by the armed forces.

The different approaches to professional education chosen by intelligence organizations from across the entire region are described below. Important differences exist in the institutional structures used, the academic level

employed, and the educational quality applied. By examining the table presented as Annex 1, the reader can more readily compare the main differences among countries and between military and civilian entities in terms of whether the schools are accredited, offer postgraduate education, and feature open access to civilians or foreign military students.

a. ARGENTINA

The Argentine Secretary of Intelligence operates the National Intelligence School (ENI). The ENI takes a mixed approach to intelligence education, as it uses an agreement with the *Universidad de la Plata* to offer a joint master's in strategic intelligence for the 21st century. The school operates within the Argentine higher-education system and it offers a general education combined with specific interdisciplinary methods useful for private or public intelligence work. The school accepts anyone interested, whether they are part of the intelligence community or not. The agreement between ENI and the *Universidad de la Plata* was suspended in 2013.

The National Intelligence Law of 2001 (Law 25520) spurred the growth of the country's intelligence education structure as a part of the national education system. Article 29 specifies that the ENI's academic offerings be subject to validation by the Ministry of Education, in accordance with the laws and regulations in effect. Additionally, article 30 encouraged ENI to collaborate with universities and think tanks.

The *Instituto de Inteligencia de las Fuerzas Armadas*, a joint services institution under the Joint Chiefs of Staff, also offers an accredited degree—a specialization in strategic intelligence analysis. This school accepts civilians as well as military applicants.

b. BOLIVIA

Bolivia's National Intelligence Office (DIE) serves as a strategic intelligence agency. It is primarily staffed by military personnel, but does have some civilian participants. The DIE does not have its own educational institution, but the Army Intelligence School provides education for most personnel.

The Army's "General Joaquín Zenteno Anaya" Intelligence School offers *Diplomados* in strategic intelligence and strategic information. This school

educates military, police, and civilian personnel with a focus on future-oriented data analysis methods. Any Bolivian with an obligation to use information or strategic intelligence to advise the decisionmaking process in public or private organizations and institutions may attend the school.

The Army's "Marshal Andrés de Santa Cruz" General Staff and Command School offers a master's in strategic intelligence, oriented to civilian as well as military personnel. It aims to improve a student's ability to analyze and produce strategic intelligence through the application of an integrated vision of national security and defense.

c. BRAZIL

The Brazilian Intelligence Agency (ABIN) has its own educational element, the *Escola de Inteligência* (ESINT)—successor to the Escola Nacional de Informações (EsNI). ESINT bears responsibility for the professional preparation of civilian and military, federal and state public servants whose organizations are bound together in the Brazilian Intelligence System (SISBIN). ESINT offers specific training programs, courses, and seminars to meet SISBIN needs.

The Senior War College offers an advanced intelligence course (CSIE), oriented toward the preparation of civilians and senior officials of the armed forces. This course allows civilian officials affiliated with federal SISBIN agencies to carry out strategic intelligence functions.

d. CHILE

Chile does not have an educational institution within its National Intelligence Agency (ANI). ANI personnel obtain specialized professional education through universities and armed forces educational institutions.

Since the end of the 1990s, several intelligence educational programs have emerged in Chile. Some have been discontinued and others have been absorbed into other disciplinary programs related to defense and security. Until 2009, the University of Chile offered a *Diplomado* in analytical methods for strategic intelligence under the auspices of its Department of Political Science and Public Affairs Institute. It had the objective of enabling professionals to contribute to decisionmaking processes in public and private institutions

through the production of strategic intelligence. The program focused on educating professionals, undergraduates in their last year of study, and military and police personnel responsible for analysis or intelligence.

The Army War College (ACAGUE) also developed a master's in military science with a three-part specialization in strategic intelligence. The first part coincided with the military science program. The second took place in the University of Chile, under its *Diplomado* in strategic intelligence. When these first two parts were completed, a mentoring program guided students in writing a thesis.

With the University of Chile's (and ACAGUE's) intelligence studies program in hiatus, the National Academy of Political and Strategic Studies (ANEPE)—a senior educational institution under the Ministry of National Defense—offers a *Diplomado* titled "The Intelligence Function in the Contemporary State," with the objective of promoting a national intelligence culture and demonstrating the importance of intelligence to the entire society.

Chilean intelligence education, whether in official government institutions or in universities, has professionalized the field, and has attracted the interest of Chile's academic community, setting the intellectual stage for expansive intelligence studies.

e. COLOMBIA

The Intelligence and Public Security Academy of the Administrative Department of Security (DAS) for many years offered specialized professional intelligence education. However, the Special Report of the DAS Commission in 2006 questioned its curriculum, the quality of its faculty, and the lack of an external review process.[661] At the end of 2011, a new National Intelligence Agency replaced DAS, and the academy was left in limbo.

The Colombian Army operates the "Brigadier General Ricardo Charry Solano" School of Intelligence and Counterintelligence (ESICI). It is a university-like institution that in 2002 gained accreditation by the National Ministry of Education. It has maintained its accreditation through self-evaluation and external review. It engages in intelligence education, professional development, and specialized training of armed forces personnel, civilians, and national and

international agencies. The ESICI offers a master's in strategic intelligence and forecasting (futurology), as well as various specializations and *Diplomados*, and it has plans to develop other master's degrees and even a doctorate.[662]

The Nueva Granada Military University also offers a *Diplomado* in strategic intelligence. It seeks to educate public and private officials, members of the armed forces, officials of the National Police (active and retired), employees of various security agencies, university students, academicians, and anyone interested in the study and analysis of strategic issues.

f. ECUADOR

In 2009, with the adoption of Public Security Law 1768, Ecuador replaced earlier intelligence institutions with the National Intelligence Secretariat (SENAIN), which reports directly to the president. As the lead element of the National Intelligence System, SENAIN prevents or neutralizes risks and threats to the state by producing and conveying political-strategic intelligence to national policymakers. Although SENAIN plans to establish a new intelligence school for the professional education of its personnel, most personnel obtain their orientation to intelligence through military intelligence training centers.

g. GUATEMALA

National Security Law 18-2008 establishes Guatemala's rules for coordinating the activities of internal and external security and intelligence institutions. The law also created the National Security Council, which oversees the National Institute of Strategic Studies in Security (INEES). This institute is responsible for coordinating and supervising the professional education and creation of expertise among public servants who attend the different governmental institutions that specialize in security training and education. The institute is charged with certifiying the professional quality of government personnel and equality of opportunity in government employment and career progression. It also oversees the establishment of a professional career system for all the organizations that make up the National Security System.

Government Accord 413-2008 regulates the State Intelligence Secretariat (SIE). Its article 46 created the Office of Professional Development and Scholarships, an administrative bureau charged with the education and

development of the professional, technical, and administrative cadre of the SIE. The same office is also responsible for developing the strategic plan for the professional development of SIE personnel. The National Institute of Strategic Studies in Security participates directly in the training and education of intelligence personnel.

h. MEXICO

Early in the 1980s, the Defense College (CD) and the Navy Advanced Studies Center (CESN) began teaching intelligence at the strategic defense level. From its start in 1989, the largely civilian National Center for Research and Security (CISEN) initiated the education and professional development of intelligence personnel through a course in national defense and a program in strategic studies. CISEN added numerous *diplomados*, courses, workshops, and seminars (which in many cases had nothing to do with intelligence).[663] Students were from CISEN and other national security organizations.

When the broad academic offerings proved inadequate to meet the CISEN's own needs, the organization began to consider the creation of a new educational structure.

> Researchers and analysts require a specialized education in intelligence and counterintelligence and in Mexico no school offers that type of curriculum; even the topic of security is practically unknown in the universities of the country. The culture of national security is in in infancy in Mexico. This means that the Center has to be self-sufficient in educating its personnel.[664]

On 16 April 2009, Mexico's official newspaper published the "Accord by which the Intelligence School for National Security (ESISEN) is established." The accord defined ESISEN as an educational institution with an academic specialty in civilian intelligence for national security. It also declared that ESISEN's educational plans and programs would be subject to approval by the secretary of education.

Even though ESISEN initially accepted as students only government employees who work for intelligence or other national security organizations, it

is expected that at some time the academic program will be available to the general public. ESISEN seeks to promote research, reflection, and a culture of interest in intelligence and national security issues among not only government institutions but among the country's citizenry. Through its technical resources, CISEN plans to make available to the school and to outside researchers various bibliographic references, documents, and other unclassified materials.[665]

The Technological Institute of Monterrey has since 2008 offered a research program in strategic intelligence within its Graduate School of Public Administration and Public Policy. This program has the purpose of studying and developing concepts and methodologies in intelligence, disseminating research findings, and promoting the adoption and institutionalization of the knowledge generated. This program also offers a course in the development and administration of strategic intelligence systems.

i. ORGANIZATION OF AMERICAN STATES (OAS)

Despite its status as an international organization, the OAS offers an educational program to develop expertise in strategic intelligence. The program is presented in the Regional Antidrug Intelligence School of the American Community (ERCAIAD), earlier named the Andean Regional Antidrug Intelligence School, established in 1999. This specialized Inter-American Commission for the Control of Drug Abuse (CICAD) center operates in Bogota, Colombia. It offers academic training in strategic and operational intelligence. Students mainly come from intelligence services, police, and other institutions involved in the fight against drug trafficking in the countries of the Andean Intelligence Group—Bolivia, Brazil, Chile, Colombia, Ecuador, Peru, and Venezuela. Other students come from Spanish-speaking OAS member countries.

The school presents mobile training courses and professional seminars in many countries of the region. Experts from France, Germany, Spain, Switzerland, and the United States, as well as other OAS members and international organizations such as INTERPOL and the United Nations Office on Drugs and Crime (UNODC) share their experiences. One course has a strategic intelligence title: "Logical structure of analysis and estimation for narcotraf-

ficking in the hemisphere to 2020." ERCAIAD's educational program has undergone a process of independent academic evaluation, ensuring its academic quality.

j. PARAGUAY

In Paraguay, the Intelligence Office (DI) of the Ministry of the Interior and the Office of Policy and Strategy (DIE) of the Ministry of Defense both have strategic intelligence responsibilities. The personnel of both offices receive professional training and education mainly through armed forces institutions.

The Institute of Advanced Strategic Studies (IAEE) has the responsibility to develop the strategic intelligence course of study (CIE), which is presented as a specialized *diplomado*. The IAEE is a public sector higher-education institution under the Ministry of Defense. Armed forces personnel currently teach the strategic intelligence courses to civilian intelligence community personnel and also to high-level state officials. The *diplomado* assists graduates in fulfilling their duties in intelligence agencies or related organizations.

CIE faculty includes instructors from the Argentine Army, provided through a cooperative agreement with the Argentine Ministry of Defense. These instructors participate alongside Paraguayan officials from diverse institutions such as the Anti-kidnapping Prosecution team, the Secretary of Money Laundering Prevention, the Technical Department for Special Customs Surveillance (DETAVE), and the Human Rights Commission.

k. PERU

Peru's National Intelligence School (ENI) is part of the National Intelligence Office and offers courses and seminars at various levels. The school's senior strategic intelligence course is oriented toward the professional development of employees of the National Intelligence Office, employees of other offices of the National Intelligence System, and the personnel of other public, non-intelligence organizations. Public Law 28664 regulates the operation of the National Intelligence System and requires that any nominee to become director of the ENI must possess at least a master's degree.

The Center for Advanced National Studies (CAEN) in Lima offers a *diplomado* in strategic intelligence for politicians, government employees, business

people, various professionals, military and police officials, and military attaches. As the most senior defense school in Peru, CAEN operates within the Policy and Strategy Office of the Defense Ministry. CAEN offers degrees in defense studies at the bachelor's, master's, and doctoral levels.

The Peruvian Institute of Public Policy, through an agreement with the Greater National University of San Marcos, offers a graduate specialization in strategic intelligence and democracy for active professionals, students in their last undergraduate year, and military and police personnel who work in the areas of analysis or intelligence.

I. UNITED STATES

Many institutions of higher education offer strategic intelligence courses and programs, some within the various security agencies of the federal government. A few civilian universities or professional schools offer intelligence degrees at the undergraduate or graduate level. Principal institutions include Loyola University of Maryland, Mercyhurst University (of Erie, Pennsylvania), the Institute of World Politics, and the Naval Postgraduate School.

The National Intelligence University (NIU) was formed in August 2011 from the expansion of the National Defense Intelligence College.[666] It is an institution of higher education with a research component, and exists to provide professional education to personnel of the National Intelligence Community, which includes intelligence specialists of the armed forces as well as civilians from the community's member agencies. The U.S. Congress authorized NIU to confer university degrees in government intelligence, and the institution is accredited by The Middle States Association of Colleges and Schools. Three degree programs are offered: a bachelor of science in intelligence, master of science of strategic intelligence, and master of science and technology intelligence.

The Central Intelligence Agency maintains the Center for the Study of Intelligence, an office that promotes study, debate, and understanding of the role of intelligence in this North American society. Sherman Kent founded the center's professional journal, *Studies in Intelligence*, in 1955.

m. URUGUAY

The National Intelligence Office (NIO) operates under the Uruguayan Ministry of Defense and does not have its own formal educational capability. NIO professional education and training takes place in purely military environments.

The Uruguayan Army's Military Institute of Advanced Studies (IMES) offers a strategic intelligence course within the army's educational system. The course contributes to the curriculum of active-duty, senior military personnel who are enrolled in the institute's general staff or basic intelligence programs. The strategic intelligence course is also available to NIO personnel and anyone engaged in some way with the country's intelligence organizations. This educational center has since 2001 maintained official recognition as a university-level institution.

The Center for Advanced National Studies (CALEN), also within the Ministry of Defense, plans to initiate its own strategic intelligence course.[667] This course will bring professional education to analysts of the Uruguayan intelligence community. The course will form part of a suite of educational offerings that will eventually lead to a master's degree in national defense.

n. VENEZUELA

Decree 7453 of 1 June 2010 established the Bolivarian National Intelligence Service (SEBIN). This civilian intelligence organization has responsibity for internal and external intelligence, in addition to counterintelligence activities. It is part of the Ministry of People's Power, in association with the Ministries of Interior and Justice. SEBIN's academic structure includes the Center for Intelligence Studies (CEI), which has the mission of designing, planning, carrying out, and supervising educational and training activities and programs. Most of its courses are at the basic level and are limited to intelligence personnel. Most training and education of civilian intelligence personnel is accomplished in the academic organizations of the armed forces.

The Ministry of People's Power also offers military intelligence courses at various levels through the Bolivarian Military University of Venezuela

(UMBV).[668] These courses are directed at military personnel and members of state security organizations. The UMBV hosts the Joint War School of the Bolivarian Armed Forces (earlier known as the Center for Advanced Military Studies), the "Brigadier General Daniel Florencio O´Leary" School of Intelligence and Psychological Operations of the Bolivarian Armed Forces, and the "Grand Marshal of Ayacucho Antonio Jose de Sucre" Institute of Advanced National Defense Studies (IAEDEN).

Summary

The foregoing survey of intelligence educational frameworks across the region reveals differences from country to country with respect to the institutional approach adopted and the level of academic recognition attained. Even in those cases where an institution has achieved official recognition, the quality of its educational outcomes remains unknown. In order to gauge the academic quality of the teaching and learning experience in any country, systematic evaluation procedures need to be in place to appraise the human-capital effects of an individual employee's educational background. This essay will now present an academic evaluation model tailored to government intelligence employees. The illustrative model should apply to the assessment of educational outcomes in intelligence organizations across the Americas.

Evaluating the Academic Preparation of Intelligence Personnel

An evaluation procedure requires carefully designed norms and objectives. Evaluation allows one to have a clear idea of how an institution performs across its sphere of action: its capabilities, its strengths and weaknesses, and the improvements that need to be made in techniques, procedures, and quality of personnel so as to attain desired objectives. Evaluation should be carried out continuously within an organization.

An evaluation plan identifies objectives, establishes what needs to be evaluated, who will evaluate whom, and what type of information needs to be collected. Further, a plan defines the purpose of the evaluation, establishes indicators and evaluative criteria, and specifies how to access and use the results. Finally, a plan addresses the preparation and dissemination of reports together with guidelines for the implementation of changes as required.

The evaluation process allows managers to identify the appropriate academic requirements for the organization's personnel, to include training and education. For the process to remain valid, representative, and useful, all personnel in the organization need to be evaluated. Evaluation can be accomplished with psychometric tests, work samples, observation, interviews, questionnaires, and any other procedure suitable for collecting data. In all cases, the means employed to collect data need to be relevant, valid, well-established, verifiable, and comparable.

A general evaluation model for an educational institution seeks to establish the degree of influence that education may have on the professional qualities of an employee. Objective measures of quality, such as the academic degrees held, may correlate with an individual's ability to apply knowledge, their efficiency, and their overall ability to perform analysis. A useful model of evaluation will help the evaluator determine the nature of any such correlations.

Figure 12 depicts a four-part evaluation process: a) curricular evaluation; b) evaluation of work performance; c) evaluation of personnel by interview; and d) evaluation of knowledge.

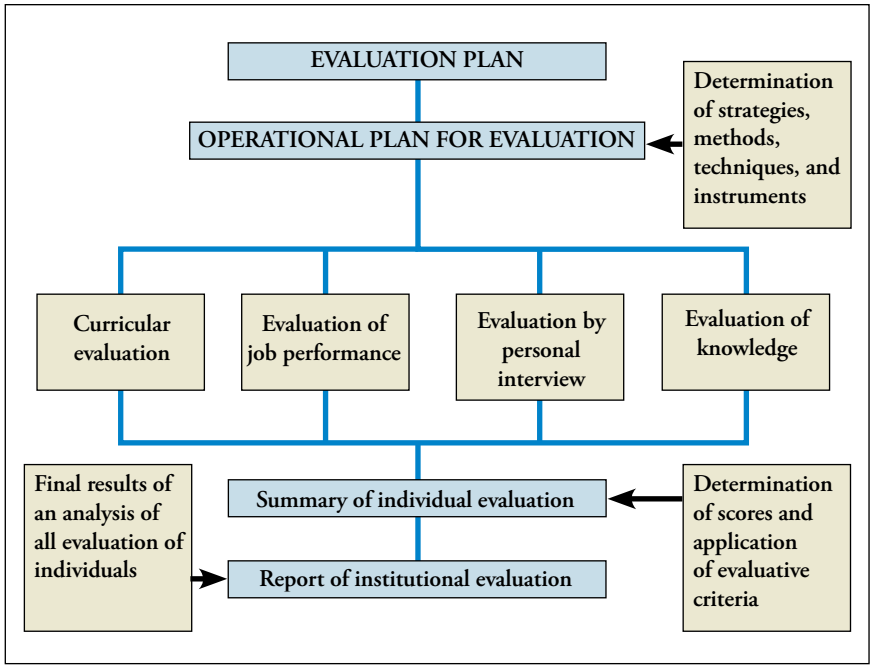


Figure 12: Outline of an Academic Evaluation Process for an Educational Institution
Source: Created by the author.

a. Curricular evaluation begins with the construction of scales that link knowledge, aptitudes, professional practices, techniques, and abilities to the academic titles, degrees, *diplomados*, certificates, and other proof of education and training undertaken. These associations are then evaluated in terms of the tasks performed by the individual, using a point system to evaluate each criterion. The evaluator will complete an evaluation form (see Annex 2) that allows for generation of partial scores for each element of education and professional development. Calculating the sum of partial scores yields the final result for this part of the evaluation process.

b. The evaluation of work performance allows one to correlate the employee's tasks and required skill set with the quality of completed work. Evaluative criteria for job performance need to reflect individual and institutional factors in the employee's productivity. The evaluation can be carried out

by the employee's immediate supervisor using criteria from the job description, with the performance evaluation for each job element depicted by a point system on an evaluation form (see Annex 3).

c. Evaluation by personal interview should prove useful in testing the job-related level of knowledge of employees, and can reveal the employee's level of performance in relation to his or her level of formal education. In a professional and institutional sense, the interviewing official can determine whether a link exists between academic accomplishments and the employee's career progression in the organization. The interviewing official should determine the importance of each factor with respect to the needs of the organization, and should document his or her opinion, taking into consideration impressions and salient aspects of the information obtained during the interview. All documentation should be distilled into the final evaluation form (see Annex 4).

d. The evaluation of knowledge determines whether the employee has command of basic subject matter, as well as more specific knowledge linked to his or her job responsibilities. This can be accomplished with a test or questionnaire that allows the reviewer to inquire about issues related to the organization, methods and tools employed in the job, and a wide variety of everyday knowledge with which a professional should be familiar. The advantage of a questionnaire is that it creates written answers, takes relatively little time, and can be completed by many individuals at the same time. However, a questionnaire needs to be designed carefully so as to obtain useful information suitable for later evaluation (see Annex 5).

To bring the process of evaluation to a conclusion, the results obtained from the curricular review, job performance, personal interview, and knowledge evaluation need to be standardized through a point system and ranked by appropriate criteria. In this way, one can give greater weight, as appropriate, to any particular evaluative criterion. The results captured in the forms already noted in Annexes 2 through 5 can be consolidated in a final summary evaluation (see Annex 6). The final report covering the entire process will benefit from cross-tabulating the data from separate evaluations with those of the entire organization, yielding a product that will allow an overall appreciation of any linkages between the academic and professional qualities of the institution's personnel. Cross-tabulation can also contribute useful insights

into the limitations of available human capital and indicate whether further professional development may be needed.

Conclusion

Intelligence organizations benefit from building human capital. The author is not alone in endorsing the practice of maintaining a professional school within the intelligence bureaucracy in any given country. In-house intelligence schools can convey specific knowledge and students can explore sensitive topics in depth in the context of a strategic vision.[669] Additionally, in-house schools can seize the opportunity to improve the functioning of the country's intelligence system through exploratory discussion and research, and by classroom discussion of professional experiences. The most advanced intelligence schools profit from a direct link with a country's higher education system and comply with curriculum review processes necessary for academic accreditation. These institutions illustrate what institutional excellence can achieve.

In some countries, a strong military influence in strategic intelligence education has coincided with a particular approach to professional development, whereby criteria for professionalism in a substantive sense have been replaced by rank-conscious tendencies and conditions more appropriate to career progression unique to purely military organizations. Nonetheless, some military-based intelligence education institutions are recognized by their country's higher education system. In these schools, civilians as well as military students—and even the public at large—tend to have access to the school's programs.

The advent of intelligence studies under the auspices of a civilian university increases the likelihood of high-quality education for current or prospective intelligence practitioners. The Peruvian specialist Alberto Bolivar Ocampo observes that "[a]n aspect of intelligence that may be considered very advanced for the region … is the availability of intelligence courses at universities. This development should overcome any remaining fears about universities being able to deal academically with a topic vital to safeguarding any country's national interests."[670]

An Ecuadorian observer notes that linkages between intelligence organizations and the academic world should be strengthened for the benefit of intelligence systems:

> [T]he capacity and potential of institutions of research and higher education are undeniable, thanks to the information they have available or that they can obtain through their institutional network of experts. In particular, they constitute a fundamental source of research in the area of strategic intelligence. The importance of these centers is linked to their transparency and academic freedom. The significance of these advantages is borne out by the information they produce (or that they have the capability to produce), especially as a result of the links they maintain with other universities and particularly with foreign institutions. Importantly, academic freedom favors the improvement of analysis, and better analysis improves the opportunity to create and provide high-quality advice.[671]

Intelligence education in universities brings a degree of democratization to strategic intelligence: it becomes more accessible to the academic world through discussion and publication. This process drives research in the field, the further development of "think tanks," and the production of theory—or its operational twin, "doctrine"—all of which permit the growth of an intelligence culture.

Individuals who work in the world of strategic intelligence require a broad spectrum of knowledge and knowledge in depth, in consonance with the elevated responsibility and complexity of their job. Hence, their education requires a correspondingly solid academic foundation. In order for intelligence professionals to reach a high level of knowledge and expertise, we cannot simply measure the number of courses or *Diplomados* accumulated. Instead, we need to insist that professionals maintain their excellence through a continuous relationship with the academic world and its Specialization, Master's and Doctoral degrees. This vision has long been sought by many in the field, even as they have been frustrated by the constant budgetary vicissitudes that have been an economic impediment to long-term planning. The lack of legislative initiatives has also played a part in suppressing opportunities to engage in this ideal approach to intelligence education.[672]

No matter what knowledge and academic titles an intelligence professional may have, he or she will always face two choices: engage in continuous

learning, or accept the onset of gradual but irreversible irrelevance. An intelligence organization should ensure that its personnel not get caught up in intellectual or academic inertia because knowledge quickly loses its currency, and educational laziness leads quickly to ignorance.

Author's Biography

Jose Gabriel Paz, J.D., Ed.M., directs the Geopolitical, Defense and Security Research Institute of the *Universidad del Salvador* (USAL, Argentina); the master's degree program in hemispheric defense and security (USAL-Inter-American Defense College), Washington, DC; and the master's degree in defense and security, Central America (USAL-National Defense College, Honduras). He teaches courses in geopolitics, international organizations, international terrorism, and transnational threats at USAL. He also serves as adviser to the Center for Latin American Economy and Trade Studies of the Chihlee Institute of Technology of Taiwan. He has completed postgraduate work in strategic intelligence at the *Escuela Superior de Guerra* (ESG, Argentina); in politics (ESG, Argentina); in national security (Galil College, Israel); and in instructor training (U.S. Army). His publications include *Bases normativas para el establecimiento de la paz y la seguridad internacional*, volumes 1 and 2 (Editorial Universidad Libros, 2000) and numerous articles, among them: "El ambiente antártico y las amenazas a la seguridad ambiental global," *Revista de la Escuela Nacional de Inteligencia*, Buenos Aires, Vol. I, Number 1, 2003. **Email:** *paz.jose@yahoo.com*.

Annex 1 (Table 15) Academic Attributes of Strategic Intelligence Educational Institutions								
Country	Civilian education center	Accreditation	Post-grad	Open access#	Military education center	Accreditation	Post-grad	Open access##
Argentina	ENI	x	x	x	IIFA	x	x	x
Bolivia					ECEME		x	x
Brazil	ESINT			x	ESG		x	x
Chile	UChile (*)(**)	x	x	x	ANEPE		x	x
Colombia	Undetermined(**)				ESICI	x	x	x
Ecuador					(**)			
United States	Several universities	x	x	x	NIU	x	x	
Guatemala	INEES(**)							
Mexico	ESISEN		x		CD and CESN		x	
Paraguay					IAEE		x	x
Peru	ENI		x	x	CAEN		x	x
Uruguay					IMES		x	x
Venezuela	CEI(**)				UMBV			

(*) Through the Chilean Army War College.
(**) Program status uncertain or discontinued.
For civilian institutions, the "open" designation signifies participation by personnel from across the government and by non-government professionals.
For military institutions, the "open" designation signifies participation by foreign military professionals. Exceptions are Peru, where CAEN is open to civilian government personnel as well as to the public at large, and Uruguay, where the IMES is open to civilian government personnel.

Annex 2 (Table 16)
Form for Curricular Evaluation (Example)

Name: ..... CLASSIFICATION
Job Description: .....
Organizational Element:.....
Date of Entry .....

Educational level	Type of degree or academic title	Scale	Number of activities	Subtotal of points
Postgraduate	Doctorate	100 pts		
Postgraduate	Master's	80 pts		
Postgraduate	Specialization	60 pts		
Undergraduate	Four-year or greater university degree	50 pts		
Undergraduate	Less than four-year university degree	40 pts		
Technical	Technical education	30 pts		
Professional development	Diplomas, Certificates, and Warrants for activities of more than one year's duration	30 pts		
Professional development	Diplomas, Certificates and Warrants for activities of six months up to one year	20 pts		
Professional development	Diplomas, Certificates and Warrants for activities of less than six months duration	10 pts		
Total points				

OBSERVATIONS: _____ _____
Accomplished by:_____ Date:_____
(The information included in this form is for the purpose of illustration only)

Annex 3 (Table 17)
Form for Evaluation of Job Performance (Example)

Name: ..... Job Description: .....
Date of Entry: .... CLASSIFICATION

Total Points Obtained			**Assignment of Grades** (Select the grade that reflects the quality as indicated in the instructions)		
			A excellent B good C acceptable D poor E unsatisfactory		
EVALUATION FACTORS	Unsatisfactory	Poor	Acceptable	Good	Excellent
					INSTITUTIONAL FACTORS
JOB-RELATED KNOWLEDGE Consider the subject's mastery of and familiarity with the duties of the job.	8 Has neither knowledge nor ability for the job.	16 Knows job, but does not master it.	24 Knows duties and carries them out satisfactorily.	32 Knows duties and excels every day in carrying them out.	40 Understands duties thoroughly and demonstrates exceptional capabilities.
COMPLIANCE WITH RULES Consider subject's mastery and familiarity with the rules that apply to the job.	8 Does not adjust to rules and lacks familiarity with them.	10 Limited compliance with rules.	12 Displays satisfactory compliance with rules.	14 Complies with rules and understands them well.	18 Exceptional compliance with rules and great comprehension of them.
RESPONSIBILITY Consider the subject's ability to quickly resolve difficult situations.	8 Requires continuous supervision because of frequent errors.	12 Requires frequent supervision.	20 Requires occasional supervision.	28 Requires supervision on certain occasions.	30 Does not require supervision.
					INDIVIDUAL FACTORS
KNOWLEDGE Consider the subjects's academic knowledge in relation to his job.	8 Has severe lack of academic knowledge.	16 Has limited academic knowledge and does not apply it.	24 Has academic knowledge and applies it in limited fashion.	32 Has sufficient academic knowledge and often applies it.	40 Has exceptional knowledge and applies it well to the job.

Annex 3 (Table 17)
Form for Evaluation of Job Performance (Example) (continued)

ABILITY TO ASSESS INFORMATION Consider the subject's ability to convey knowledge, ideas, and suggestions.	8 Finds it difficult to analyze issues and draw conclusions.	16 Often has difficulty in analysis and conveying ideas.	24 Fully analyzes issues as assigned.	32 Satisfactorily analyzes all the issues related to job	40 Excels in analyzing issues related to job and evaluates with accuracy.
ANALYSIS Consider subject's use of intellectual abilities for systematic analysis of information.	8 Lacks capability to do analysis.	12 Displays limited ability to do analysis.	24 Carries out analysis adequately.	32 Has an elevated capability to do analysis.	40 Analytical capability is exceptional.
					PERFORMANCE FACTORS
ABILITY TO COMPLETE TASKS Consider subject's performance of his duties.	8 Slow to complete tasks and often does not finish them.	16 Completes tasks to get them out of the way.	24 Completes tasks satisfactorily.	32 Shows desire to accomplish tasks.	38 Eager to address tasks.
QUALITY OF COMPLETED WORK Consider subject's application of knowledge, experience, and attention to detail.	8 Often commits errors and work is unsatisfactory.	16 Work has limitations; needs improvement.	24 Work accomplished acceptably.	32 Accomplishes work with care and attention to detail.	40 Exceptional, high-quality work; improves continuously.
AMOUNT OF WORK COMPLETED Consider the volume of work the subject typically accomplishes.	4 Little work accomplished.	8 Less than optimal amount of work accomplished.	16 Acceptable quantity of work accomplished.	20 Makes an effort to complete extra work.	24 Continuously strives to increase amount of work accomplished.
OBSERVATIONS: ----------					
Completed by:_____ Date:_____					
(The information included in this form is for the purpose of illustration only)					

Annex 4 (Table 18)
Instructions for Personal Interview

Use of the interview guide:

To prepare yourself for the interview, review the specific personnel forms, and develop the set of general and specific questions to be asked during the interview. In the interview guide, establish the number of questions to be generated and prepare additional, pertinent questions. Proceed in accordance with the interview guide, using the introductory questions for each area and other selected questions. Mix questions and statements and use comfortable phrasing to reduce the appearance of this being an interrogation. Present the questions in condensed form to save space.

Use of the subject evaluation section:

Evaluate the subject on the principal factors using your own judgment. When the interview is complete, convert your notes into a formal evaluation. As you do this, determine the importance of each factor in light of the work requirements. You should document your impressions and the most relevant information points in the spaces labeled "comments," "notable qualities," "weak points," and "overall summary." Pay particular attention to the notable qualities and the weak points that relate to the critical requirements of the job. Then, transfer your evaluation of the subject on each factor to the summary evaluation table.

INTERVIEW GUIDE

1. Tell me about your intelligence work experience from your first job to your present position. I'd like to know for each job what you did, what you liked about it, what you didn't like about it, your salary, and any special achievement.

2. What level of academic degree do you have? Have you been able to apply your academic work to your job?

3. What knowledge from your academic study has been of most use for your job? What knowledge should you have to make yourself more useful to the profession?

4. Can you give me one or two examples of how your academic knowledge was useful in your job?

5. Does your academic knowledge allow you to work more effectively than others who work with you but who do not have a similar academic preparation?

6. Do you think the organization in which you work values the academic credentials that you have? Have you experienced greater professional growth as a result of having the academic qualifications you do have—are they reflected in promotions, recognition or increased salary?

7. Do you think a correlation exists between academic degrees held by an employee and his or her ability to work well with other government employees, with academics, or with counterparts in other countries?

Annex 4 (Table 18) Form for Personal Interview (Example) (continued)	
I. General information	**CLASSIFICATION**
Name:	
Job Description:	
Date of Entry:	
Ii. Personal interview	
CRITERIA:	
Presentation, up to10 points : (Measures activity and personality)	( )
Security and Persuasiveness, up to 20 points : (Measures comprehension and ability)	( )
Rationality, up to 10 points : (Measures analytical ability)	( )
Adaptability, up to 10 points : (Measures suitability for work)	( )
Knowledge, up to 20 points : (Measures specific knowledge in relation to the workplace)	( )
III. Evaluator's considerations	
Comments:	
Notable qualities: ..... ( )	
Weak points: ..... ( )	
Overall summary: ....., ...	
Points:	
ASSIGNMENT OF GRADES	
(Select the grade that reflects the overall summary) **A excellent** **B good** **C acceptable** **D poor** **E unsatisfactory**	
Completed by: _____	**Date:** _____
Signature of Subject: ……	
(The information included in this form is for the purpose of illustration only)	

Annex 5 (Table 19)
Form for Evaluation of Knowledge (Example)

Name: ..... CLASSIFICATION

Job Description: .....

Date of Entry: .....

		Reply to the following questions:	**Points**
1	Is strategic intelligence a science or an art? Explain your opinion.		
2	What technological tools for knowledge management are you familiar with? Describe them.		
3	What is the current concept of national security?		
4	What are the ethical foundations of the profession? Provide examples.		
5	Describe the significance of "strategic surprise" in a diplomatic sense.		
6	How is a country's national culture related to national, strategic intelligence?		
7	In light of prevailing legal norms, what are the characteristics, attributes, and limitations of the organization to which you belong?		
8	What is the function of the Fourth Department of the General Staff of the People's Liberation Army of China?		
9	What relationship exists between strategic intelligence and strategic opportunities?		
10	Dialogic, recursive, and hologramatic principles are part of a particular way of thinking about problems. Identify and describe this way of thinking.		
Total points			

ASSIGNMENT OF GRADES **(Select the grade that reflects the overall score)**	
A excellent	
B good	
C acceptable	
D poor	
E unsatisfactory	

OBSERVATIONS:

Completed by:_____ **Date:**_____

(The information included in this form is for the purpose of illustration only)

Annex 6 (Table 20)
Form for Summary of Individual Evaluation (Example)

General information **CLASSIFICATION**

Name: ....

Job Description: .....

Date of Entry: .....

I. Curricular evaluation
POINTS EARNED: .....

II. Work performance
POINTS EARNED: .....

III. Personal interview
POINTS EARNED: .....

IV. Evaluation of knowledge
POINTS EARNED: .....

FACTOR	VALUE	
1		
2		
3		
4		
Subtotal		

Final point total from individual evaluation process:

Assignment of grades (Select the grade that reflects the overall score)	
A excellent	
B good	
C acceptable	
D poor	
E unsatisfactory	

Annex 6 (Table 20) Form for Summary of Individual Evaluation (Example) (continued)
OBSERVATIONS: ---------- ----- Completed by:_____ Date:_____ (The information included in this form is for the purpose of illustration only)

Source: All Annexes/Tables compiled by the author.

Managing Intelligence Information for Multinational Cyberspace Security— Approaches by the United States and Brazil

Robin M. Rogers

"The legal and policy entanglement in cyber is far, far more difficult than it is in some of the other domains."

—William Lynn III[673]

Setting the Stage

Every day, news reports claim that some government, company, or group of citizens has been "attacked" through cyberspace. Cyberspace can be a dangerous place, but sensationalized reports can evoke a response out of proportion to the actual event. Cyberspace attacks do threaten national security, economic security, and even personal security. Some persons responsible for cyberthreats act on their own; some act as part of a criminal gang or political activist group; and some act as agents of a foreign power—either to conduct espionage or "military operations."

Intelligence managers can take advantage of coordinated efforts among the private sector, law enforcement, military, and intelligence communities to defend cyberspace. Information sharing, whether from proprietary, law enforcement, or intelligence soures, contributes the essential ingredient for coordination. Obstacles to sharing information include uncertainty over what specific information to share and what can or should be shared. These obstacles are compounded when countries need to share intelligence information with each other.

From an intelligence manager's perspective, this essay reinforces the importance of information sharing, first by exploring the role of common terminology and language conventions, then highlighting the threat that actors in cyberspace pose to national, economic, and personal security. Actions taken by the U.S. and Brazil to respond to the cyberthreat illustrate the challenges to intelligently managing intelligence information. The essay

concludes with an exploration of potential improvements in cybersecurity information handling policies and practices.

Coming to Terms with the Cyberspace Threat

Merely describing the threat can become a vexing problem. Intelligence managers regularly use terms from very different cultures—from the worlds of military, intelligence, and law enforcement specialists. Additionally, various private-sector cultures (including the Internet industry), news-media cultures, and even cybersecurity cultures all use different terms to describe the same thing—be it an unremarkable event or an impending threat. Conversely, representatives from these cultures may use the same term to describe very different things.

A logical place to start this exploration is to define cyberspace itself. In the United States alone many different definitions coexist. The *Cyberspace Policy Review* described it as the "globally-interconnected digital information and communications infrastructure"[674] Yet that very document further defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[675] An information technology (IT) website defines it as a "metaphor for describing the non-physical terrain created by computer systems."[676] Another site from the Czech Republic uses similarly fuzzy terms: "Cyberspace is currently used to describe the whole range of information resources available through computer networks."[677]

Bypassing other characterizations of cyberspace, this essay will employ a more precise definition: "Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected information-communication technology (ICT)-based systems and their associated infrastructures."[678] It may seem that this definition uses too many words to describe a "virtual" entity. One reason to use it is that it can apply to many of the cultures mentioned earlier. It applies to things—"electronics" and "systems" and "infrastructures"—and touches on the way people "exploit" those things to create and use information. The definition stops just short of including information itself as part of cyberspace.[679]

Defining cyberspace helps us to understand what happens there. This essay focuses on two of the negative things that happen within that space: attack and intrusion. Paraphrasing one online source, "A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter how a computer is set up to handle logic or data, and can result in data compromise or cybercrimes, such as information and identity theft."[680] Though this definition may serve some of the communities mentioned above, it does not work as well for military or intelligence communities because an "attack" of any sort may lead to military action, including war. In this essay a "cyberattack" is the use of cyberspace to disrupt, deny, degrade, destroy, or manipulate information resident in computers and computer networks, or the computers and networks themselves.[681]

Law enforcement organizations, such as the U.S. Federal Bureau of Investigation (FBI), use a concept more inclusive than "attack"—they prefer the term "cyberintrusion."[682] Although the FBI does not provide a standard definition, by implication cyberintrusion refers to "accessing a computer (or network or system) without authorization or exceeding authorized access, and by means of such conduct obtaining information."[683] This definition focuses on gaining unauthorized access. Though the U.S. National Institute of Standards and Technology does not specifically use the term "cyberintrusion," it does refer to "network intrusion" and also uses that term to refer to unauthorized access to networks.[684]

Private computers, networks, or systems[685] may convey or contain classified national security information. In other cases, that private information may be intellectual property or proprietary. In still other cases, the private information may be personal account information, email, or photos.

In the latter two cases, the cyberintrusion constitutes a cybercrime. In the first case (stealing classified or other national security information) the action should be considered cyberespionage. Espionage is a crime as well; the difference between cyberespionage and cyber crime generally determines which organs of government bear the responsibility for protecting against the act or prosecuting those who commit the act. Law enforcement organizations typically have responsibility for deterring and prosecuting cybercrime. Counterintelligence organizations, which may be part of law enforcement, military,

or intelligence communities (in any combination) usually handle cases of cyberespionage.

In thinking about intelligence information that supports national efforts to defend against the threat of hostile operations in cyberspace, whether an attack or an intrusion, understanding who is responsible for defense becomes important. Intelligence organizations need to be familiar with the information needs of the organizations they support. The need to work with both counterintelligence and law enforcement organizations introduces additional cultures, and therefore additional information needs, to the responsibilities of the intelligence manager.

The idea of "attribution" similarly concerns any intelligence manager responsible for supporting cybersecurity efforts. Attribution determines "the identity or location of an attacker or an attacker's intermediary."[686] Identity would include personal identifying information, such as a name, identity number, account information, or alias. The location may be either virtual or physical. Note that the citation also mentions intermediaries—those entities through which an attacker (or intruder) passes on the way to the target. Intermediaries may be witting or unwitting; determining their complicity adds to the task of establishing attribution.

The variety of sources cited for the few definitions mentioned above reminds the intelligence manager of the many cultures with an interest in defending cyberspace. Sharing information among these various cultures in such a manner that it can be understood by the recipient as well as the originator presents a challenge. An intelligence manager would certainly know that differences in language (Portuguese/English) and culture (Brazilian/United States) affect information sharing. How to achieve a common understanding of the concepts used to characterize threats from hostile cyberspace operations also demands a manager's attention.

Recognizing Cyberspace Threat Concepts

All too often, a *threat* in cyberspace is equated with an *effect* created there. To avoid this confusion, intelligence managers, like managers in other cyber communities, can disaggregate the concept with a standard threat formula: intent + capability = threat. By this formula, anyone with the capability to

cause a negative effect must also have the intent to use that capability in order to become a potential threat.

The Low Orbit Ion Cannon (LOIC) illustrates how a tool can allow an actor to change from being a potential to an actual threat. Used for legal purposes, the LOIC is a tool that tests how well a network can stand heavy activity loads. Used as a cyberattack weapon, it can overload networks to the point of making them crash, thus creating a denial of service. The LOIC is free to download and a YouTube video shows viewers how to use it.[687] This means that virtually every person using the Internet can gain the capability to conduct a cyberattack or cyberintrusion. Capability is not a limiting factor.

In cyberspace, intent requires a nuanced understanding. A botnet[688] capability allows a person to remotely control many other computers (or even networks). Gaining control of computers is generally a cyberintrusion, unless the owners of the controlled computers have consented to being controlled. Either way, the resulting botnet represents a capability. The person controlling the botnet may want to cause a distributed denial of service (DDoS) attack. Or he may intend simply to use the botnet to facilitate unauthorized access to other computers, information, or networks. In the first case, the effect is a cyberattack. In the second case, the effect constitutes a cyberintrusion. A cyberintrusion may have occurred when the botnet was simply created. The threat in both cases is the actor, not the effect.

Given that understanding, intelligence managers may either provide or gain information about three categories of threats. The first is the state actor; the second a nonstate actor; and the third a lone actor. As experience has shown, these categories are not exclusive—an actor operating in one category may also operate in another. An actor's allegiance complicates an intelligence manager's decision to share information about threats in cyberspace: once personal attribution has been established, is it possible to draw a connection to a larger set of actors?

For many years, private cybersecurity companies, together with government IT, law enforcement (LE), and intelligence organizations ranked nation-state actors as the top cyberthreat. In many ways, this characterization remains accurate. The U.S. Computer Emergency Readiness Team, US-CERT, claims that nation state

> programs are unique in posing a threat along the entire spectrum of objectives that might harm U.S. interests. These threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption. Among the array of cyberthreats, as seen today, only government-sponsored programs are developing capabilities with the future prospect of causing widespread, long-duration damage….[689]

Even out-of-date estimates indicate that more than 120 countries have or are developing cyberattack or intrusion cybercapabilities.[690]

Some nondemocratic states may use their capabilities against what they perceive as internal threats, whereby their intent affects the nature of the threat. Other state actors use cyberintrusions to gather national security information. The U.S. Secretary of Defense, Leon Panetta, confirmed in 2012 that China employed cyberintrusions to gather classified information from U.S. Department of Defense computers and systems.[691]

Nonstate actors appear in many varieties. Cybercriminals, motivated by greed, may come to mind first. Cybercriminals tend not to engage in cyberattacks, except in cases of extortion. Cybercriminals conduct intrusions mostly to obtain data or access to financial account information. Such activity may target individuals within one country, although the Shadowcrew "organization" conducted intrusion operations on a global scale from 2002 to 2004, stealing credit information or identities of individuals from numerous states.[692] A publication by PricewaterhouseCoopers Brazil Ltda identified cybercrime as the second-leading criminal activity in Brazil in 2011.[693] The Internet security company Norton, in its Cybercrime Report for 2011, pegs the total net cost of cybercrime in the United States for 2011 at $139.6 billion, while the net loss worldwide was $388 billion.[694]

Most cybercrime in leading countries occurs in the private sector, with private individuals as common targets. Cyberintrusions against national security targets (classified information, information held either by governments or by government contractors) are usually not the work of cybercriminals, but are

sometimes conducted by nonstate actors such as patriotic hackers operating from China or hacktivist groups such as Anonymous or Lulzsec.

An example of nonstate actors conducting cyberintrusions appears in the "face off" between Chinese patriotic hackers and those from the Philippines over fishing rights off Scarborough Shoal (or, as the Chinese refer to it, Huangyan Island). Chinese patriotic hackers, protesting against the Philippine government after its Navy tried to arrest Chinese fishermen for illegally fishing in the area, disrupted Philippine government websites. These actions came not from Chinese government offices, but from Chinese patriotic hackers acting on their own.[695] Though these "patriotic hacker" nonstate actors certainly engaged in criminal behavior, they generally do not do so for criminal gain.

Hactivists make up another nonstate group that poses a threat of hostile action in cyberspace. Although hacktivists have been conducting intrusions for several years, the threat they pose has become almost equal to that of some state actors even if their motive is different. *Wired* magazine has reported that hacktivists outperformed cybercriminals in 2011.[696] The cybersecurity company Kaspersky placed the rise of "hacktivism" as the top new threat for 2011.[697] Hacktivists such as the Anonymous and Lulzsec groups have the attention of both law enforcement and national security communities.

Anonymous operates as an amorphous collection of individuals who seek to protest what they consider objectionable, such as the Church of Scientology, or the efforts to stop Wikileaks.[698] Their protests may appear in the form of directed denial of service (DDoS) attacks, where a particular site, server, or computer is inundated with either email or requests to the point of shutdown. Other protests involve defacing a website; they often replace information or images with claims about their own abilities. Other cyberintrusions steal information such as account owner's names, emails, or other personal information. These protests generally occur at a global scale. Much of this group's activity could be considered cybercrime as it is directed against private organizations.[699] Anonymous claims to have disrupted the websites of various British government organizations, an action that crosses the threshold from criminal to national security threat activity.

Lulzsec is a much smaller group of individuals (hacktivists) who have less defined goals (or no goals at all beyond having fun creating mayhem), but who

use the same tools as Anonymous to express their views through cyberspace. This group claims responsibility for various intrusions and attacks. Known intrusions include theft of user and administrative data from Sony websites. The motivation in that case was to demonstrate the company's faulty cybersecurity.[700] Lulzsec also claims to have used DDoS to attack various Brazilian government websites,[701] the website of an FBI-affiliated organization called Infraguard,[702] and the publicly accessible website of the U.S. Central Intelligence Agency.[703] Like Anonymous, Lulzsec can pose a challenge to both law enforcement (the intrusion into Sony and Infraguard) and national security communities (the attacks against the Brazilian and U.S. government sites).

A third source of hostile action in cyberspace is the individual actor—sometimes called a hacker. An example of a lone actor is Kevin Mitnik, once described as one of the most wanted computer criminals in the United States.[704] Mitnik was accused of gaining unauthorized access to a number of computer companies and systems and stealing the credit card information of over 20,000 people worldwide. Mitnik claimed that his motivation in all of his hacking activity was to "learn, not to cause harm."[705]

An attack (such as a DDoS) may be seen as a criminal act or as an act subject to the Law of Armed Conflict, thus inviting a military response. A tool used to carry out a DDoS attack may be the same tool used to deny customers access to their bank accounts or to deny a military commander access to his deployed forces. Yet the appropriate response to the use of that tool should vary dramatically. Legal and policy decisions (both national and international) should determine the response. Intelligence managers, law enforcement officials, or private cybersecurity firms should be able to provide information useful to the necessary legal and policy decisionmaking.

An intrusion poses similar challenges, but intelligence managers face even more uncertainty with respect to sharing information about this action. Both attacks and intrusions start with a threat actor gaining unauthorized access to a system or network. In some cases the tools and vulnerabilities used for an intrusion also generate an attack. Determining the intent of the threat actor becomes the key to differentiating one from another, and sometimes the determination cannot be made until the attack (or intrusion) has occurred. Since the action itself should determine the response, it sometimes remains

difficult to know if law enforcement or military defense forces should be responsible for prevention or incident response.

The Intelligence Manager's Assessment of Cyberthreats

An effective intelligence manager must have a set of requirements against which to work. Those requirements (some may call them information needs) will guide the manager in knowing against whom collection should be tasked and just as importantly, knowing who has expressed the need. Knowing who wants or needs the intelligence information can help one understand why the need exists, who else might want or need the intelligence information, and how (in what format) to deliver the information.

Legal, academic, government information technology, and private-sector cybersecurity observers have provided differing opinions about who within and outside government should have responsibility for protecting against threats of hostile action in cyberspace. Questions that frame the debate include: 1) Who is responsible for protecting the nation's national security information and critical infrastructure, and what *is* that infrastructure?; a corollary to this question is, Who will establish rules of engagement for offensive and defensive actions against cyber opponents?; 2) Who is responsible for protecting the infrastructure that societies find necessary now that their very operation relies on secure cyberspace, and just what is *that* infrastructure?; 3) Who is responsible for protecting intellectual property?; and 4) Who will protect access to private information associated with identity documents or bank accounts? Intelligence managers should not answer such questions—but they could benefit from knowing the answers so they can provide the appropriate level of information to those who are responsible.

This essay cannot answer all those questions, but as a discipline that has proactive information collection, information handling, and analysis at its core, and the responsibility to develop strategic assessments for national leaders, intelligence and its managers are favorably positioned to provide an initial understanding or net assessment of cyberspace conflict. Further, because the U.S. Intelligence Community has a strong program for assessing external as well as internal threats and opportunities, and one's understanding of the familiar is often improved by reference to a less familiar, but similar set of

circumstances, this essay will examine the status of Brazil's cybersecurity arrangements as a way to improve understanding of the U.S. situation.

In 2001, the U.S. Congress recognized the need for protecting cyberspace when a new law found that "[p]rivate business, government, and the national security apparatus increasingly depend on an interdependent network of critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors."[706] That interdependent network is cyberspace. The World Bank reports that in 2010, 75 percent of people in the United States, and slightly over 40 percent of the population of Brazil, were active in cyberspace.[707]

Many governments lease commercial communications lines, and even commercial devices. The U.S. military relies on some leased telecommunications lines[708]—and those lines are part of the cyber domain. Thus military and critical infrastructure data can easily be on or pass through the same bit of cyberspace as intellectual property information from a private company, or a private citizen's bank account information. In the United States, personnel and agencies responsible for protecting cyber infrastructure include the Departments of Defense, Homeland Security, Justice, and Commerce, as well as the overall Intelligence Community.[709]

Seven U.S. national cybersecurity centers support the intelligence, defense, civilian, and law enforcement/counterintelligence communities of the U.S. government. At least three of them also provide support and guidance to nongovernment users.[710] Figure 13 shows the centers, which communities they primarily belong to, and their respective authorities and responsibilities. It also lists the functions carried out by each center.

Note that these centers do not directly include any commercial or academic cybersecurity organizations or companies. U.S. CERT and the NCCIC (through, in part, regional and topical Information Sharing and Analysis Centers-ISACs) do provide information to the Internet industry and other private-sector entities, and the NCIJTF provides support to other law enforcement and regulatory agencies. Through coordination, any of the centers may provide information useful to the others. However, the NCCIC has the overall responsibility to coordinate information sharing. Representatives from

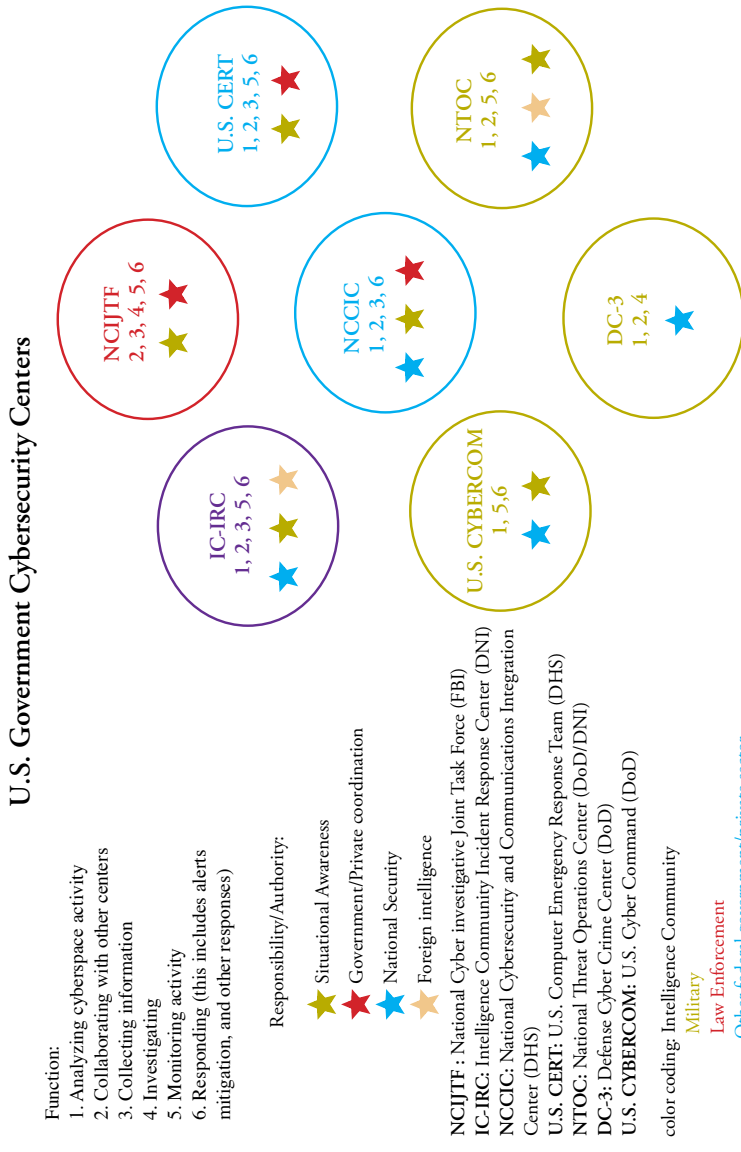


Figure 13.
Source: Developed by the author. Data are from 2012.

Figure 14.
Source: Developed by the author. Data are from 2012.

the U.S. Department of State work in these centers to handle international aspects of cybersecurity.

An intelligence manager answering similar information needs for the government of Brazil also faces a complex challenge. Just as in the United States, many organizations provide cybersecurity for the government and society. Figure 14 shows some of those organizations, their functions, and their responsibilities. CERT.br, the Brazilian Computer Emergency Response Team, functions much like US-CERT.[711] SERPRO, a public/private company, provides data processing for many of the civilian parts of the Brazilian federal government.[712]

The Brazilian Federal Police acts as the primary law enforcement organization for cybersecurity,[713] although Brazilian state police also participate in cyberspace law enforcement.[714] The Brazilian Federal Prosecutor's Office and the Ministry of Justice handle prosecution of cybercriminal activity. These two have responsibilities similar to the U.S. FBI. The federal government's Center for Cyberdefense (CDCIBER) protects the military and governmental network, as well as Brazilian information infrastructure as a whole.[715] The Brazilian Army created and manages this organization, which has responsibilities similar to those of the U.S. Cyber Command. The Brazilian Institutional Security Cabinet (GSI) serves a function parallel to that of the U.S. Intelligence Community. The Brazilian Intelligence Agency (ABIN), a civilian organization, operates within the GSI.[716] Finally, the Department of Information and Communications Security (DSIC) provides cybersecurity for the Brazilian government's executive branch.[717]

The illustrations of U.S. and Brazilian cybersecurity efforts highlight the overlapping interests of the various organizations responsible for addressing hostile action in cyberspace. Although some parallel structures exist, lines of communication and information sharing differ markedly. The lines are virtually nonexistent for Brazil, while the number of lines between U.S. centers may generate so much information sharing that the detection of repetitive, circular reporting can become a problem.

In an interview, General Jose Carlos dos Santos, the commander of CDCiber, indicated he was working to establish close ties with GSI, as well as SERPRO.[718] Such efforts are apparently not universal across all communities, however.

A civil police cyber expert, Emerson Wendt, commented that the Brazilian Internet Steering Committee (CGI.br) simply receives information, and does not share it with other organizations with cybersecurity responsibilities.[719] CERT.br, an organization subordinate to CGI.br, has responsibility for computer security incident reports in Brazil. Its role and authority in providing threat warning remain unclear, however.[720]

Like an intelligence manager supporting U.S. efforts to defend cyberspace, a Brazilian intelligence manager has the opportunity to anticipate and make sense of cyberthreats, taking into account the country's disparate institutional arrangements established to handle various aspects of current and future cyberattacks and intrusions. A Brazilian intelligence manager faces a less complex information-sharing infrastructure than his counterpart in the U.S., it appears.

Managing Cyberspace Security from an Intelligence Perspective

The illustrations of cybersecurity centers in the U.S. and Brazil give us some idea of the overlap of interests, authorities, and responsibilities encountered in defending cyberspace. Questions that surround an attack or intrusion are of course numerous, and include, among other things: What happened after unauthorized access was gained? Was something altered or stolen? Was it a repeat of an earlier event? Do we know the computer code (or tool) used? The intelligence manager should know the answers to many of these questions (and other related ones) so that he or she may wisely manage the intelligence actions needed to suppress ongoing incidents or to prevent future events. Intelligence agencies responsible for cybersecurity can expect to interact with the entire set of centers in their respective countries. The interaction requires a two-way exchange of information.

A hypothetical scenario will help illuminate the dynamics of an actionable cyberevent in the context of the diverse institutional cybersecurity environment of Brazil and the United States. (To ensure that this scenario is clearly hypothetical, it will refer to countries A, B, C, etc., and individual or groups of cyberintruders 1, 2, 3, etc.) Suppose that a group of intruders (#1) gained unauthorized access to a government website of country A (and the databases linked to it). Once it gained access, the group started downloading

information as well as changing the website. The intruder group (a loose alliance made up of individuals from countries A, B, C, D) then sold or gave away some of the database information to other intruders (# 2, #3, and #4), in countries E and F.

The changes to the website at first seemed nothing more than defacement, but government cyber investigators discovered that some data were destroyed. The defenders also found two programs the intruder group left behind. One would automatically log information about anyone who visits the website and send it to a server in country C. The other program would attempt to take control of any government computer whose user downloads a particular file. The government cyberdefenders were able to immediately deactivate the two leave-behind programs.

Some of the databases contained personal information on government employees as well as private citizens. Some contained information used for government policy development, and some also contained information about government contracts with companies that support national defense, law enforcement, and a national health service. Finally, some of the databases contained system administrator data, including passwords that allow varying levels of access to the databases. Although nothing in any of the databases was marked "classified," some of the government policy and contract information was and is "sensitive." Government employees and private citizens would be concerned that their personal information had been accessed without authorization.

Impetus to Share Cybersecurity Incident Information

Because this scenario involves a domestic as well as a foreign threat to country A's government, to the private sector, and to private citizens, all of the communities discussed in this essay will need to learn enough to protect their future operations in cyberspace. As the discussion shows, each of the four communities (intelligence, military, law enforcement, and private sector)—which, for this essay, includes the entire Internet industry—will initially have only partial knowledge of the case.

As key players, intelligence managers will want to know who intruded so that they could monitor for future activity of the foreign actors that make up intruder group #1, and of the other intruders—ideally to provide warning of future intrusions. They would want to know what happened—sufficient

details of the attack to allow them to look for other indications and associations that may help them understand why the intrusion occurred. The "what" in this case might be the tools and tactics the intruders used as well as the metadata about what information was in the databases. The actual information within the databases would probably be beyond the authority of intelligence managers to acquire, but may be accessible to counterintelligence organizations. Intelligence managers would want to know the "why" as well. This might give them a better picture or estimate of the level of the threat to national security.

The military community, and in particular military intelligence, would be interested in the event for several reasons—not the least of which is the nature of the access to defense contract information gained by the intruders. They would also certainly be interested because the intruders destroyed data, meeting the definition of an attack. If the military community were responsible for a national CERT beyond its own networks, then the need for detailed information becomes even broader.[721]

The law enforcement (LE) community, and especially any specialized unit focused on developing intelligence, has perhaps the broadest information needs in this scenario. They need to know whom to prosecute and what evidence may be useful in court for developing a motive and leads for criminal prosecution. The LE community needs details about what happened so it can determine what laws have been broken. Since there are both foreign and domestic members of intruder group #1, the LE community would deal with both national and international courts in attempting to prosecute. The LE community need for information on all related intruders may depend on the cyber laws in country A.

The private-sector community may seem to have the least diverse information needs in this scenario, but that initial judgment may be misleading. For example, who the intruders are may or may not be important from an immediate response viewpoint, but what happened and why certainly are. The private sector at large, and especially government contractors, would also want to know what was downloaded just as it would want to know what tools and tactics were used. What was downloaded would be important from an operational as well as a legal standpoint. Tools and tactics information would allow the private sector to be better prepared to protect networks within its

own purview. Depending on that purview (and the laws in country A), the cybersecurity offices of the private sector might also need to know some details about the personal information that was stolen, to be able to alert those individuals to the fact of the intrusion.

Knowing what the various cybersecurity communities need to know, and why, remains the critical foundation for sharing intelligence information. It allows intelligence managers, who will tend to have the broadest overview of the incident, to know what information to try to gather—which can allow them to know what sources to look for and what methods to use to gain information from those sources. However, impediments do exist to the smooth and unrestricted gathering and sharing of information, even by national intelligence agencies.

Impediments to Sharing Cyberintelligence Information

Just as intelligence managers have an obligation to gather and share a broad range of information, they also have an obligation to protect both the information they gain[722] and the sources and methods used to obtain it. The second obligation can complicate meeting the first. The scenario above can be used to frame a discussion of some aspects of that complication.

An effective intelligence manager should ensure that his organization has legal access to a variety of sources of information. Some of that information may be openly gathered and thus may not be classified. Gaining information from other sources may require clandestine or covert methods. Sometimes the source of the information may determine the level of classification and even the way that information is handled. Sometimes the information itself, regardless of the methods used to gather it, will determine the classification. And sometimes, it is the combination of the two that may require a higher classification. In addition to the restrictions that come with classifying information, most intelligence managers will also face restrictions on sharing it widely, especially outside of an intelligence community.

In the case of the scenario above, an intelligence agency may gather intelligence information about who was a part of intruder group #1, as well as the identity of intruder #2 and #3. This information may have come from sources and methods that require a medium-level classification as well as some sources that require the highest-level classification. The agency also may have gathered

information on the tools and tactics that the intruder group used. The tools and tactics information may have come from the highest-level sources; and in addition the information must be handled through special means.

The point of classification and dissemination restrictions is to safeguard information, sources, and methods. Thus, only those with access to the appropriate security levels should be able to obtain the information. In most governments, high-level national security advisers or ministers would have the clearances and authorizations needed to see all the information on intruders #1, #2, and #3, plus the details of their tools and tactics. However, information at the highest levels of classification and authority may not be available to most members of the military, the LE, or private-sector communities. That is why cyberincident information should be handled by specialized intelligence units of the military and LE communities made up of individuals with high-level intelligence information access, to ensure that all potentially relevant data are available in their respective operating environments.

In the absence of specialized military or LE intelligence personnel or units, what can an intelligence manager do to help satisfy the information needs of those without high-level clearance levels and additional authorizations? One approach to answering this is described in a U.S. Intelligence Community Directive:

> Utility is maximized when customers receive or are able to expeditiously discover and pull or request intelligence, information, and analysis in a form they are able to easily use and able to share with their colleagues, subordinates, and superiors. WMU [write for maximum utility] ensures intelligence, information, and analysis are produced in a manner to facilitate reuse—either in its entirety or in coherent portions—thereby enabling wider dissemination and enhancing its usability.[723]

The concept of WMU describes a goal rather than an action. Another section of the directive refers to "sanitization," implying that it is one of the actions that may achieve the goal. However the directive does not define "sanitization." Sanitization removes source or method information that originally

required marking/handling at a high security level, so that intelligence information may be reported at a lower security level. The directive does require that "[s]anitized products should never render facts or judgments in a manner inconsistent with their higher-classified version—facts, judgments, confidence levels, and probabilistic language must be congruent."[724] Keeping all this in mind, intelligence managers should be able to provide varying levels of detail about the activity described in the scenario, depending on the security access level of the intended recipient. This technique may apply both to national and to international sharing efforts.

An intelligence community may not have the authority to share intelligence information with the private sector. In the United States, most members of the Intelligence Community are authorized to share intelligence information only with other federal agencies.[725] Any sharing with the private sector risks the appearance of favoritism if government information reaches only some representatives of the private sector.

Sharing Cyberintelligence Information Internationally

Many countries have specific information-exchange agreements with others. Most are community-to-community agreements; that is, military-to-military, law enforcement-to-law enforcement, and intelligence to intelligence. With respect to the scenario presented, country A may have an agreement with country C to share information between law-enforcement communities, but not necessarily between intelligence communities. The private sector also shares information internationally. Of course, some parts of the private sector operate internationally, with interests and information gathering capabilities in many foreign jurisdictions.

Many countries belong to multilateral organizations. In the illustrative scenario, all members belong to the Organization of American States (OAS), which has established information-sharing agreements involving a number of the communities discussed in this essay. Further, it has a cybersecurity strategy that outlines the importance of information sharing—not only sharing information about a threat, but also about cybersecurity practices within member states. This strategy was created by an OAS secretariat for legal affairs working group and specifically addresses the issue of trust:

> Since much of the information that CSIRTs [Computer Security Incident Response Teams] need to exchange is proprietary or otherwise sensitive, trust must be developed among the participants as an essential element of the hemispheric network. To build such trusted relationships, CSIRTs should be created to possess … a secure infrastructure for managing sensitive information; the ability to communicate securely with stakeholders; and procedures to guard against inappropriate disclosure of information. Member states will always maintain the right to decide on the type of information that will be exchanged through their designated CSIRTs.[726]

This document, and the philosophy it embodies, closely parallels the approach suggested above, whereby within an individual country, specialized intelligence units in military intelligence and police intelligence organizations facilitate sharing of intelligence information about cyberincidents.

Exploring Potential Improvements in Cybersecurity Information Sharing

National cyberspace security has become more than a "whole of government" issue—it is an all-of-the-nation concern, and as such poses severe challenges to those who need to share threat information, especially intelligence specialists and their managers. The intelligence community typically leads a country's capability to monitor the foreign context in which criminally or ideologically based cyber capabilities and intentions take form. With this breadth of responsibility, it is only logical that the most thorough exploration of potential improvements in information-sharing policies and practices throughout the cyberdefense system would be undertaken from an intelligence perspective.

The preceding discussion of intelligence information sharing about the threat of hostile action in cyberspace addressed current policies and practices—at least in general terms. But what if intelligence managers could influence those policies and practices? What might they choose to influence? The following points take into account the idea that some aspects of these recommendations may already be practiced, but have not yet been formalized or institutionalized.

1. Build flexibility into the intelligence requirements process. In the United States at least, the formal intelligence requirements process works fairly well; it establishes a consumer's needs and seeks to explain their importance, then prioritizes the needs. However, at times an intelligence service may legitimately discover something of great importance, but which has not yet been identified as a need. Intelligence requirements processes must be flexible enough to accommodate that prospect.

2. Consider whether the Intelligence Community should have authority to monitor the threat of hostile activity in cyberspace within the United States. Of course, the political contest between security and privacy or freedom will provide the ultimate answer to this question. Society itself will need to resolve where that balance is struck. Can an intelligence manager ethically and morally influence the society's decision? Perhaps—if in no other way than by informing society of the threat and establishing trust. It does appear that the Intelligence Community, with its existing legislative and judicial oversight arrangements, can suitably exercise that authority.

3. Treat cyberspace as a culturally distinct domain. "Changing the culture" of information sharing within a bureaucracy is one of the easiest things to say and probably one of the hardest to accomplish. One of the things intelligence managers can do is to share as much as laws, policy, and regulations allow. Another thing intelligence managers must do is to explain, in understandable terms, why they can or cannot share.

- What to share (and at what security level)? In the United States, current policy establishes what information must be classified, how it is handled, and who may see it. At issue, to some, is whether existing laws and rules are being appropriately applied to cyberspace-related intelligence. At least one authority finds that the role of intelligence in cyberspace needs to be defined and implemented differently. General Michael Hayden, former director of the National Security Agency and the Central Intelligence Agency, recommends that we ask a series of hard questions about cybersecurity and the protection of information in this domain. For example, "What constitutes a 21st century definition of a reasonable expectation

of privacy?"[727] In that light, intelligence managers might benefit from a general reassessment of the concept of privacy and private information in cyberspace. As General Hayden says, "Google and Facebook know a lot more about most of us than we are comfortable sharing with the government."[728]

- With whom to share? An ever-increasing number of potential customers seek intelligence information on cyberspace threats.
    - Current restrictions forbid intelligence managers from sharing with certain subsets of customers (federal to state, local, or tribal sharing). Good reasons support this approach for most intelligence (such as the federal vs. state's rights debate over who pays for or regulates what), but for cyberspace threats, the situation is different. Physical boundaries mean little in cyberspace, and the logic of symmetry suggests that a sound defense against cyberthreats likewise should not be restricted geographically through a differentiation between internal and external threats.
    - Sharing intelligence information with members of the private sector is difficult to do, and may be forbidden. Some reasons for not sharing in this case seem understandable: the problem of how to avoid showing favoritism and the existence of differences in trustworthiness of some establishments over others. However, an important synergy will be attained when intelligence managers can share equally with the private sector and the federal government. U.S. Senator Dianne Feinstein has encouraged President Obama to make changes in this area. She urged the creation of an executive order that would "direct the Intelligence Community and the Department of Homeland Security to provide as much information as possible to the private sector about cyberthreats, including classified information."[729] The British Government Communications Headquarters has developed a program called "Cyber Security Guidance for Business" to establish cooperative information sharing between British intelligence and the British private sector.[730]
    - Sharing cyber-security information multilaterally, never an easy prospect, should be greatly helped by a clarification of rules for internal

sharing within individual countries. This objective can be understood and promoted by addressing the final question below.

4. Identify an existing intelligence, law enforcement, or defense agency or create a new one to centralize the security and defense of cyberspace across public and private domains. Currently, for anyone dealing with the threat of hostile action in cyberspace, knowing who is in charge of information collection, analysis, and cyber-threat identification and legal prosecution appears impossible, given so many national communities, each with different responsibilities and leadership. If intelligence managers could influence any executive branch policies and practices, they should recommend the establishment of a central authority for cyber defense. Whether it be the law enforcement, intelligence, or defense community, someone needs to be in charge. Laws, executive orders, policy guidance, and regulations need to act on this recommendation so that all communities can identify their role in defending the nation—and its allies.

In any country, the central entity would need three sets of authorities or responsibilities (or their equivalent): foreign intelligence, law enforcement, and regulatory (rule-setting). In the United States, an organization that already has this set of authorities and responsibilities is the U.S. Coast Guard. Perhaps that organization, in the way it manages its intelligence, law enforcement, and regulatory responsibilities, could serve as a model for a cyberspace security organization. The Coast Guard was effective in combining intelligence capabilities together with law and regulatory enforcement responsibilities during the Prohibition Era in U.S. history, when a high volume of illegal alcoholic beverages entered the United States as contraband from near-shore vessels, an activity often coordinated by organized criminal groups.[731]

Equally as important, the central agency will need to establish and maintain trust among U.S. citizens:

- Trust that personal privacy and national security can be complementary in practice, rather than always at odds as separate and competing deals. Society must determine that it can trust the government to monitor certain activity in cyberspace, at levels that might at least approach what the private sector currently monitors. The government (especially the agencies responsible for cyberspace security)

must maintain society's trust that it will protect privacy as established by the laws that society accepts.

- Trust that the government and the private sector can work together to share information. This too is a two-way street. Government must trust the private sector to protect sensitive information. The private sector must trust that the government will protect intellectual property and proprietary information. Both must trust that the other will use shared information for the purposes intended by law and policy.

Author's Biography

Robin M. Rogers holds a master's degree in strategic intelligence from the Defense Intelligence College (now the National Intelligence University) and another master's in history from the University of Maryland. He served in the U.S. Air Force for 30 years, retiring as a colonel. Subsequently, in the Department of Defense, he worked in intelligence as an analyst and teacher of analysts before moving to a corporate policy position. As a faculty member at NIU, he has used his combined intelligence, cyber, and policy experience to develop the cyberspace operations curriculum for the University. **Email:** *Robin.Rogers@dodiis.mil*.

Harnessing Security Sector Intellectual Capital: Transforming Advisor Situational Awareness into Sociopolitical Understanding in a Smart Power Environment

William S. Brei
Nathalie J. Frensley
Killaurin O. Roberts

> "[A]s this 'Afghan Surge' draws down and more financial and political constraints kick in, we're going to have to seriously empower mentors as an organization. Their tactical social advantages with their counterparts will have to be fused into real operational impacts. Otherwise, the Alliance's strategic goals will become a thin eggshell and the nations will just start pointing fingers."
>
> —NATO Operational Mentor and Liaison Team (OMLT) Commander's remarks during Cigar Night, October 2010, Afghanistan

The OMLT commander's informal remarks refer to the complexities facing all advising efforts, from district to ministerial levels, in the smart power environment of Afghanistan operations. These complexities, as we explain below, stem from both host- and donor-nation sovereignty issues that, on the one hand, intensify the need for greater sociopolitical understanding of host-nation partners, but on the other create obstacles and tighter restrictions to obtaining it. In this essay, we present the Sociopolitical Network and Behavioral Analysis Team (SNBAT) construct, employed in Afghanistan from 2010 to early 2012, in support of a multinational effort, ministerial-level advising team tasked with building capacity and capability of the Afghanistan National Security Forces (ANSF).[732] We offer the SNBAT construct as a straightforward strategy and model for Security Sector Reform (SSR) advising missions to gain sociopolitical understanding of their host-nation counterparts in today's politically charged smart power environments.

Particularly in a smart power multinational effort, we observe a tendency for the advised host-nation's political relationships and actions to be relatively independent and autonomous, in line with their often-assertive statements

about maintaining sovereignty.[733] As we explain below, understanding the social and political forces that affect a host nation's security partners in such an environment is crucial for the success of SSR advising missions. In the past, intelligence organizations would have provided advising missions with this environmental information. However, as we further explain, application of the smart power approach has created circumstances that cause intelligence organizations to encounter tighter restrictions on their activities. Part of the reason for these restrictions stems from host-nation sovereignty considerations, but the difficulties of multinational intelligence coordination also contribute. Additionally, the politically sensitive nature of the advising mission itself prevents intelligence organizations from providing or appearing to provide secretive, in-depth sociopolitical information or analyses to advisors, for fear of losing the trust of host-nation partners. Thus, the advisor corps in a smart power environment needs to solve the problem of how to meet its own pressing situational understanding needs in a mission requiring face-to-face engagement with high-level representatives of the host nation.

We address this problem within the framework of intellectual capital. Capturing, compiling, developing and preserving an organization's intellectual capital are the means to transform it into a learning organization. The SNBAT strategy, in an advising mission context, is to apply strategic management of intellectual capital to enable an advising mission to carry out what have traditionally been military and civilian intelligence functions without the negative mission hazards that come with participating in a centralized intelligence bureaucracy. The nature of a SNBAT wholly and solely within the advising mission helps to ensure confidentiality of what are simultaneously personal and professional relationships for advisors, even as the team combines individual advisor information to create a coherent, bird's-eye view of the advising mission's sociopolitical environment.

The authors draw from their experiences with the Afghan National Army Development (ANA DEV), a multinational ministerial advising element of the NATO Training Mission–Afghanistan (NTM-A), to suggest how advising missions in smart power environments can create an *organic* intellectual capital management capability to capture, preserve, and coherently combine advisors' sociopolitical insights and experiences and enhance mission effectiveness. By capably connecting the unconnected, capturing know-how in

context, delivering information and insights directly to the point of execution, and adopting a long historical view–the four elements of the ANA-DEV SNBAT's intellectual capital development–sociopolitical understanding is created from advisors' situational awareness.

Smart Power and the Demand for Sociopolitical Analysis in Military Advising Environments

U.S. Special Forces have historically carried out the responsibilities of advising foreign security forces. A recent consequence of the rise of smart power in U.S. foreign and national security policy is the increased participation of conventional forces[734] in SSR advising, particularly at the national (ministerial) security force levels.[735]

Smart power "underscores the necessity of a strong military, but also invests heavily in alliances, partnerships, and institutions of all levels to expand American influence and establish legitimacy of American action."[736] The smart power approach combines coercive and inducive "hard" types of power, on the one hand, with attraction and co-option "soft" types of power, on the other.[737] Smart power's emphasis on alliances, partnerships, and institutions necessarily requires viewing national sovereignty less in terms of relative gain (zero-sum, win-lose) and more so in terms of absolute gain (variable-sum, win-win).[738]

Security sector development–the full range of activities undertaken by a nation and its partners to improve the way it provides safety, security, and justice to its citizens[739]–is a key smart power activity.[740] Security sector reform reestablishes or reshapes "*institutions* and key *ministerial* positions that maintain and provide oversight for the safety and security of the host nation and its people" [our emphasis].[741] Security sector *advising*, particularly at the ministerial level, emphasizes the soft side of smart power because advisors must "persuasively articulate suggestions to their … counterparts" in lieu of "directly implementing changes necessary for SSR."[742] Indeed, "advisors' success depends on their ability to convey recommendations in a manner that makes change acceptable to their advisees."[743]

Smart power has three components: fusion of military, diplomacy and development powers,[744] promotion of democracy and a market economy,[745]

and participation in multilateral operations with increased United Nations engagement.[746] Each component affects the operating environment of security sector advising. Security sector advising takes place in an environment of democracy promotion, typically where accountable and transparent governance has broken down and where democracy building may be unpopular with local power brokers. In Afghanistan, smart power multilateralism takes place within the NATO alliance structure, which in turn operates under a U.N. mandate. Various unique requirements[747] complicate the command and coordination of multinational advising missions.[748] Security sector development takes place in conflict, postconflict, and/or weak state environments in which host-nation military and civilian authorities are to coordinate plans and actions alongside international community military, diplomatic, and development officials who likewise are to coordinate their actions.[749]

Figure 15: The Advising Mission's Complex Operational Environment
Source: Created by the authors.

Smart power expands the scope and level of understanding that ministerial security sector advisors need about the sociopolitical and behavioral environment in which they work. Some specific elements of that environment include:

- Their counterpart's individual histories and their formal and nonformal relationships within the host nation's security organization;
- The security organization's history and formal and nonformal relationships within the wider governmental power structures, including other government ministries and units;
- The social history and relationships within and between societal groups, including civil society, economic, and religious actors.

The human face of these general requirements is illustrated in the following vignettes.

An advisor was frustrated about the amount of time a counterpart spent in meetings with individuals from outside the Afghan National Army (ANA) and the Ministry of Defense (MoD). The counterpart had spent almost the entirety of his military career at one of the ANA's training schools, starting prior to the Afghan-Soviet war. His career history gave him the unique ability to vet claims of former mujahidin who sought to join the ANA at credited rank based on earlier service prior to the Soviet-Afghan war. When this was brought to the advisor's attention, it became clear that the general's "social visits" to discuss events that happened more than three decades before were in fact very important duties for ensuring professionalism, given the loss of official records during Afghanistan's many conflicts. This advisor also now realized that this general was a unique resource for understanding the history and evolution of ANA doctrine, maneuver, and training.

The International Security Assistance Force (ISAF) insisted that a very well-connected individual at the center of a high-profile scandal be removed from duty, and received assurances that would happen. An analyst outside of ANA-DEV wrote a widely circulated report alleging that one MoD leader was a participant in the scandal because of his apparent slowness in following through on those assurances. The analyst did not take into account that the MoD leader, of the same ethnicity as the individual to be removed from duty, was securing the support of clan elders for the latter's removal and thereby preempting appeals to clan loyalties to reverse the decision. Moreover, the MoD leader and the individual to be removed were in different political factions within the ethnic group. Additionally, the analyst did not take into account that Afghan social norms prevent "firing" a colleague who is a peer in status or an ethnic compatriot; however, it is permissible to move them laterally to another position.

One counterpart had been demoted to a lesser position within the MoD a few years prior by the president, leading advisors to regard him as no longer a powerful player among the military leadership. The current advisor found out, however, that this individual was the senior elder of a historically influential tribe. Additional research suggested that throughout Afghanistan's modern history a disproportionately high number of civil servants were drawn from this tribe. In this instance, the counterpart's influential tribal status overshadowed and robustly compensated for what was a demotion only in office.

Sociopolitical insight allows an understanding of reasons that may lie behind a counterpart's actions that seem to have no purpose except to stall and delay. Such insight also points to the "influentials" who "can get things done" within an authority structure that remains obscure to an outsider. In short, advisors with deep understanding of the operating environment, as opposed to superficial awareness of culturally appropriate conventions of social engagement, are able to capitalize on social knowledge.

Of Mice and Mousetraps: Understanding an Advising Mission's Unique Information and Knowledge Management Needs

Upon its inception, ANA-DEV assimilated several organizations that had over the previous decade contributed to advising and mentoring the Afghan Ministry of Defense (MoD).[750] Advisor-produced individualized quarterly ministerial development plans (MDPs), with defined objectives, milestones, and measures of success, were established to monitor and evaluate progress toward professionalization of the Afghan MoD's many assistant ministers' offices, staff sections, and special units.

As part of quarterly evaluations, advisors were expected to produce what were referred to as "Human Terrain Maps" about their counterparts. ANA-DEV advisors had a wealth of information and insights about the sociopolitical environment. However, advisors lacked information and analysis support to place or corroborate their insights into deep historical context and/or relationally into the social networks of the sometimes-changing contemporary political, social, or religious environments. Additionally, the "Human Terrain Maps" were restricted to one slide and structured to produce non-networked "ego" charts or Venn diagrammatic representations of very broad social grouping

information. Opportunities were lost to combine individual advisor awareness of the bits and pieces of their counterpart's sociopolitical environment into a larger, more comprehensive advising mission organizational situational understanding of the Afghan MoD as a professionalizing security organization, as a security organization within a political governmental environment, and as a politically potent governmental security organization within Afghan society.

Worse than the lost opportunities resulting from the "Human Terrain Mapping" shortcomings was the evaporation of advisors' insights about and influence with their counterparts once their tours of duty ended. At the time ANA-DEV had no in-house knowledge management capability to capture and retain their unique sociopolitical and behavioral information. Without capture and retention of advisor information, a corporate body of advising knowledge could not be developed for second-, third-, and fourth-generation advisors. Afghan counterparts saw for themselves the overall lack of corporate, cumulated knowledge and recognized the weak, beginner's level of awareness of their sociopolitical realities on the part of most new advisors. From the advisory perspective, to use a mouse and mousetrap analogy, ANA-DEV did not seek to capture and retain information for the sake of building a mousetrap database as would be the case for a formal intelligence organization; rather, ANA-DEV saw its advisors' prospective intellectual capital as a means to build a more resilient and knowledgeable mouse in a turbulent and changing environment.

The Uniqueness of Information from the Advising Relationship

Individual ANA-DEV advisors typically spent one year in Afghanistan. During that year, an advisor would spend between 15 and 40 hours per week with counterparts, depending on the closeness of the relationship. Sometimes advisors would travel with their counterparts. Some advisors built rapport based on the respect shown by having made an effort to advance beyond elementary proficiency in the Dari or Pashto languages. The ample time an ANA-DEV advisor spent with a counterpart typically provided tremendous visibility and opportunity to gain insights about a *single individual's* decisionmaking and behavioral tendencies, shaped by historical events, political influence, and clique and factional memberships within the MoD and ANA, Government

of the Islamic Republic of Afghanistan, and wider Afghan society. Few who serve in Afghanistan, including intelligence analysts working at the large forward operating bases, have as much visibility and contact time with senior Afghans as do the advisors to the Afghan National Security Forces (ANSF) Ministries of Defense and Interior.

An advisor's daily work provided access to freely available yet singularly unique insights about *their individual counterpart*. For example, advisors sometimes worked with their counterparts on developing policies. MoD policies have both signatures and signature blocks. MoD ministers' signature blocks can provide, to those willing to translate from Dari or Pashto, a complete name, from which it is possible to identify not only family but subtribal and tribal or clan affiliations, education accomplishments, preferred forms of address, and sometimes commands or offices held. In some cases the signature blocks contained statements about exploits or aspirations. Additionally, because signature blocks were self-written by the Afghan counterpart, they served as a "social presentation of self"[751] in ways conventional resumes could not.

The uniqueness of an advisor's insight comes from gaining and holding a counterpart's trust. This has two consequences. First, insights developed from an advising relationship makes them inherently sensitive, but not because of the nature of any given insight. Rather, advisor insights are inherently sensitive because if a counterpart perceives a lack of discretion on the part of the advisor, trust and respect in the relationship will erode. A second, related consequence is that a great many advisors, though eager to analyze the sociopolitical environment and their counterpart's role in it, resist engagement with intelligence organizations out of concern for how the information embedded in their dialog will be used outside the advising mission. Many advisors at NTM-A self-identified as "correctors, not collectors," and their avoidance of intelligence organizations intensified as the infamous Wikileaks episode unfolded.

Unpacking the Problem: The Strategic Management of Advisors' Intellectual Capital

When mentors and advisors, such as the OMLT Commander, asserted that "tactical social advantages … will have to be fused into real operational impacts," ANA-DEV leadership understood it to mean compiling an individual

advisor's awareness and insights into a greater comprehensive understanding of MoD's organizational, sociopolitical and behavioral environment. ANA-DEV leadership did not see the comprehensive understanding gap as a problem caused by advisors' lack of learning and applying advising principles and techniques, initial country-specific knowledge, or experience in Afghanistan. Many uniformed service members who advised had multiple previous tours in Afghanistan. Many contractor advisors had spent three or more years in Afghanistan. ANA-DEV leadership highly valued the knowledge advisors brought from their predeployment preparation, including the extensive language and country-specific training given to Afghanistan-Pakistan Hands (APH) and the Ministry of Defense Advisors (MoDA).[752] Quite the opposite, ANA-DEV leadership, in the words of a Canadian colonel, saw that "too much unorganized, untapped advisor information, rather than too little, is preventing the advising mission from becoming a learning organization."

Since the rise of the knowledge and information economy in the mid-1990s, strategic management of intellectual capital and organizational learning have been recognized as central to an organization's competitiveness and meeting its goals efficiently. The introduction of an influential volume on intellectual capital notes that

> [i]n part, management's challenge is to orchestrate the transformation of raw intellectual material generated by individuals into intellectual capital–knowledge packaged in forms that can be invested directly in the same spirit as the firm's hard assets… Organizations possess immense unstructured storehouses of informal know-how, which in the absence of intellectual capital programs is distributed in a haphazard fashion across the minds of individuals and a plethora of recording media such as memos, books, voicemail messages, paper files, and databases. And even less-tangible intellectual assets are embedded implicitly in the workings of the organization itself–in its culture and in its informal routines and processes. By more deliberately forming intellectual capabilities from this sea of unstructured intellectual material, management can more readily invest such capital in opportunities targeted to meet strategic knowledge requirements.[753]

Intellectual capital and organizational learning are separate but related components of organizational adaptation to an unpredictable external environment. When a process for converting intellectual capability into organizational capital is in place, a learning organization may emerge. Such an organization facilitates learning by its members and continuously transforms itself.[754] It does so by capturing the insights generated by its different components at the operating level and forging those insights into shared corporate knowledge across the organization.

Strategic management of intellectual capital to foster a learning organization has three general characteristics. The first is "connect[ing] the unconnected," by providing an informational foundation for "creating and linking communities...with similar interests and tasks."[755] In an advising context, this involves compiling each advisor's insights and knowledge derived from each individual advising relationship into a mission's overall understanding of the advising environment. When this is accomplished, advisors begin to improve their understanding of the larger systems and processes that constrain their counterparts' actions.

The second is facilitating "the capture of know-how in context ... [because organizations] pragmatically cannot … require professionals to address general questions about their knowledge as a process outside normal workflows. [Organizations] need to build…knowledge that embodies the[ir] particular contexts…."[756] Applied to advising, this means that a mission's intellectual capital must have competencies and maintain currency of policy knowledge about the security institution, the advising process, and the interactions between the two as well as knowledge about the wider sociopolitical environment of the security institution.

The third element of strategic management fosters a learning organization's "capturing intellectual capital in context [and] delivering it directly to the point of execution. Well-formed, investible intellectual capital is of relatively little value unless it is delivered to where it is needed at the time it is needed."[757] For an advising mission, this third characteristic underscores the need for the intellectual capital capability to originate within and be dedicated to the advising mission in order to ensure its value for organizational learning.

An additional, fourth element that fosters organizational learning is compilation of the organization's historical institutional knowledge in addition to its current knowledge. Different organizations have varying strategic goals and needs, with some, such as advising missions, having to be at the extreme edge of adaptation to external environmental changes. For advising missions, those changes can include domestic politics in the advisor's home country, alliance/coalition politics, and host-nation politics as well as the evolution of professionalization and capability of the counterpart security sector institution. In the highly uncertain environment of a security sector advisory mission, that mission's organizational learning needs will most closely resemble those of organizations that face strategic renewal. A strategic renewal context places additional needs on a learning organization, requiring renewing "organizations [to] explore and learn new ways while concurrently exploiting what they have already learned."[758]

For an advising mission engaged in assessing "normal" versus "abnormal" reactions to change in turbulent environments, its knowledge requirements demand that its capability to manage its intellectual capital take a relatively long historical view in contextualizing and compiling advisor knowledge. For this and the previous three reasons, it is most unlikely that an entity outside of the advising mission could successfully manage advisors' intellectual capital in such a way as to contribute to reforming the mission into a learning organization.

Building ANA-DEV's Intellectual Capital: How an Advisor's Situational Awareness Is Organically Transformed into an Advising Mission's SocioPolitical Understanding

The central question ANA-DEV faced in becoming a learning organization narrowed to "How can an effective *understanding* of the MoD's sociopolitical environment be created out of the *situational awareness* possessed by the combination of individual advisors, particularly in a context of abundant data and information?" Although similar questions are central to the work of many professions, including those of the academic and the development worker, perhaps not surprisingly this question has been intensively studied in the context of intelligence analysis itself. The United Kingdom Ministry of

Defence Joint Doctrine Publication 2-00 (JDP 2-00), "Understanding and Intelligence Support to Joint Operations" has grappled most directly with doctrinally answering this foundational question.[759] Nonetheless, as explained below, the combination of advising's unique needs and constraints on intelligence analysis prevents even this valuable emergent direction from meeting advising mission needs in smart power environments.

JDP 2-00 frames *understanding* as "refer[ing] to the acquisition and development of knowledge to gain insight (knowing why something has happened or is happening) and foresight (being able to identify and anticipate what may happen)."[760] Achieving understanding demands our "developing the most inclusive perspective of an actor, group, environment, or situation."[761] Situational awareness, "the appreciation of what is happening, but not necessarily why it is happening"[762] necessarily comes first, but it alone remains an insufficient step toward gaining understanding. However, we can observe that an "analysis of situational awareness provides greater comprehension (insight) of the problem."[763] With early comprehension of the problem, "judgment based on comprehensive insight"[764] (in the sense of being able to estimate logical relationships between causes and consequences of the problem) can provide the foresight that leads to being able to identify anticipatory scenarios.

JDP 2-00 distinguishes understanding from situational awareness by ascribing to *understanding* a "level of analysis and depth of comprehension that allows judgment to be applied effectively."[765] Applying this construct to an advising mission requires two minor modifications. These modifications apply to limitations of any analysis support from outside of the advising mission to meet the advising mission's sociopolitical information and understanding needs.

First, when an advising mission engages with a ministerial *institution*, it is actually, through its many individual advisors, sequentially engaging with their respective *individual counterparts*. Consequently, advising mission contexts involve multiple counterparts who are socially networked or otherwise grouped among themselves but who each have an advisor with an exclusive focus on them. To understand the social networks and groups within the advised ministry, there is a need for an all-encompassing *scope of comprehension*– a fusion of the insights of *all* advisors–in addition to the depth identified and emphasized by JDP 2-00. Scope of comprehension in addition to depth of

comprehension brings us back to the intellectual capital need to connect the unconnected and to take the long historical view.

Second, JDP 2-00 places emphasis on identifying the appropriate level of analysis. However, for this construct to be relevant to an advising mission, there is the need for multiple levels of analysis to better understand the simultaneous ministry organizational, governmental and societal influences on an individual counterpart's behavior. This corresponds to the intellectual capital principle of capturing know-how in context.

Consequently, the application of JDP 2-00's concept of *understanding* to an advising mission calls for increased attention to multiple levels of analysis and the greater *spatiotemporal scope of comprehension* that allows judgment to be applied effectively.[766]

The following diagram provides an example of the progression from initial situational awareness to understanding of the sociopolitical, relational and behavioral dynamics that affect a ministerial advising mission.

Situational Awareness
The appreciation of what is happening, but not necessarily why it is happening

"My counterpart is young, highly experienced and a brilliant general but says he won't be promoted because of his ethnicity. The figures on Ministry ethnic balance show they are on track. Why is my counterpart worried?"

— question posed by a well-trained, insightful adviser who appreciates the situation and recognizes the need to obtain insightful understanding.

Analysis
Developing the most inclusive perspective on an actor, group, environment, and/or situation
Key Question: Is there a significant relationship between age and ethnicity in the Ministry?

Age by Ethnicity Contingency Table		Ethnic Groups		
		A	B	C
Age by your Groups	31-40	10	5	15
	41-50	20	20	10
	51-60	20	30	10
	61-70	50	5	5

Comprehension: Insightful Understanding
Why something has happened or is happening

Ethnic Balance % (Target 50/30/20)	A	B	C
Overall	50	30	20
31-40 Year Group	10	8	38
41-50	20	33	25
51-60	20	50	25
61-70	50	8	13

Relationship between ethnicity and age group is established (Chi-square = 58.08, df=6, Yates Chi-square = 52.3) by analysis and the problem is comprehended: Although total aggregate ethnic balancing targets have been met, the Ministry remains ethnically imbalanced within age groups.

Multiple Levels of Analysis

Scope of Comprehension:
All advisers' information on age and ethnicity of their counterparts

Foresightful Understanding
Being able to identify and anticipate what may happen

Ethnic Imbalance within age groups may mean that intergenerational mentoring between counterparts is not happening as needed for capacity-building to take hold.
Not factoring ethnic balance into advising assignments may mean unwitting reinforcement of ethnic imbalance in the Ministry.

Judgment
Estimation of logical relationships between causes and consequences of the problem

Multiple Levels of Analysis

Is this caused by
- *governmental interference in Ministry attempts at ethnic balance?*
- *societal tribal or clan influence on the military?*
- *leadership indifference to future officer cohorts?*
- *some other social dimension or factional influence that is being balanced in lieu of ethnic balance?*

Figure 16: Bridging the Gap between Situational Awareness and Understanding in a Hypothetical Security Sector Reform Problem
Source: Reflection on authors' field experiences.

In this hypothetical example of an emergent ethnic balancing problem within a security ministry, the first of five steps in bridging the awareness-understanding gap starts with a single well-trained advisor's situational awareness item. The advisor's counterpart makes a statement that the advisor recognizes as unusual when expectations are that ethnic balance policies are succeeding. The counterpart's concern, given his qualifications and age, is recognized by the advisor as a possible problem due to the latter's relationship with the counterpart and operational knowledge of the advising mission's planning and milestones for ethnic balance. The advisor, because of proximity and relationship with the counterpart, is also making an expert assessment as to whether the counterpart's concern is out of personal self-interest or a loss of confidence in the ethnic balancing component of professionalization and capacity building. (Intelligence) analysts outside of the advising mission, who do not have both the advisor's detailed, expert knowledge of the relationship and the operational advising mission, are unlikely to recognize the counterpart's statement as an indicator of a potential systemic ethnic balancing problem. Further, an outside analyst typically remains removed from the rapid tempo and quick adjustments that are an inevitable aspect of a fielded advising mission.

The second step is analysis and it requires, as in all analysis endeavors, identifying the most inclusive perspective of an actor, group, environment, and/or situation in order to correctly identify the research question. In this example, the advisor recognizes the need to understand whether the counterpart is motivated merely by personal ambition only or by professional concerns about ideals of fairness and professionalism within ethnic balance policies. Answering the advisor's question requires far more information than any insight gleaned through only one advising relationship. To develop the necessarily inclusive perspective requires a scope of comprehension that encompasses *all* advisors' insights on their counterparts' ages and ethnicities.[767]

This is easier said than done. Determining age of counterparts is not as straightforward as one might assume. Oftentimes, official biographies do not contain this information (although signature blocks–discussed above–can and do contain clues). Detailed knowledge of rank advancement patterns in the old army prior to security force assistance as well as knowledge of historical events–not always well known and documented in resources available in the West–are helpful to estimate age if an advisor feels it would be

inappropriate to ask confirming questions. Another complication is that the counterpart's age of record in ministry records, which in some countries affects retirement and promotion status, may differ from actual age and be more important. A final–and the most important–complication is how to identify meaningful boundaries for bracketing age groupings. Militaries grow and cut their troop strengths as a matter of the "guns versus butter" domestic political competition for funding–as we are seeing in the United States today. Sometimes militaries have meaningful boundaries for age groupings based on military campaign eras–for example, in the United States, references to "Korea," "Vietnam," "Pre-9/11," "Post-9/11" and others—are heavily laden with professional experience, career progression, and doctrinal emphasis meanings. Other countries' militaries are no different.

If it is difficult for advisors to grapple with these issues regarding counterpart age, it is even more so for analysts outside of the advising mission. This is because scope of comprehension–connecting the unconnected and taking the long historical view in an advising mission context–requires access to all advisors' insights about all counterparts *that advisors may not realize they actually have*. Outside analysts, without having themselves acquired operational understanding of the advising mission, will not know how to help advisors realize their insights. A second problem lies in spatio-temporal depth of analysis, in that knowledge of locally published national, regional, and pre-reform army histories, along with understanding how to identify tribe and ethnicity subgroups and factions (such as from signature blocks as discussed above) and the ability to read the counterpart's language are important for assisting an advisor in realizing and articulating the insights they do have about their counterpart. Depth of analysis–capture of know-how in context in this advising example–will be more narrow and specialized. In this hypothetical example, answering the "age question" will involve expert knowledge about the ministry's personnel, promotion, and merit policies.

The third step is comprehension, which yields insightful understanding. Comprehension is closely related to analysis but differs from it in that additional comparisons or data manipulations are carried out to better refine the understanding of why something has happened or is happening. Consider the tables in the diagram above. In this hypothetical example, the Age by Ethnicity contingency table was produced by aggregating all advisors'

information about the age and ethnicity of their counterparts (and, when necessary, carrying out additional research to estimate age). However, these findings would not empower advising mission leaders with the insightful understanding of how this could occur, despite the overall totals meeting ethnic group percentage targets for balancing. To provide that insight, the overall ethnic balance proportions need to be compared with ethnic balance proportions broken out by age group.

Getting to the step of comprehension in a ministerial advising context will often require the capture of know-how in context about functions that are far removed from the threat concerns of (intelligence) analysts outside the advising mission. In this example, the identification and understanding of ethnic imbalance being obscured by aggregate totals requires knowing about and having access to information on the ministry's personnel, promotion, and merit policies and procedures. The expert source of that knowledge and information will in fact be the advising mission itself, *which makes the outside analyst more dependent on the advising mission than the advising mission is dependent on outside analysis to produce comprehension*.

Understanding is achieved with the fulfillment of comprehension. However, comprehension's insightful understanding is about why something is or has occurred. To anticipate what may happen beyond the initial occurrence requires the fourth step of judgment, by which we mean estimating the logical relationships between causes and consequences of the problem.

A ministerial-level advising mission engages with a security-sector institution, which is an organization with internal dynamics affected by external societal and governmental dynamics (see the first diagram above). The advised security ministry organization will have multiple "constituencies" located within the multiple levels of the organization (soldiers, corps commands, subordinate commands, headquarters, etc.), the government, and the society. Consequently, a ministerial-level security sector reform mission needs multiple, simultaneous levels of analysis in order to consider all possible locations at which causes and consequences of the problem can occur. The fourth step of judgment, with its emphasis on multiple levels of analysis, makes possible foresightful understanding, the fifth and last step in progressing from situational awareness to understanding. Foresightful understanding refers to being able to identify and anticipate what may happen, given the logical

relationships identified between causes and consequences of the problem. As with judgment, foresightful understanding depends on multiple levels of analysis. However, analysts outside of the advising mission may be organized to focus their work at only a single level (strategic, operational, or tactical) rather than at multiple, nested levels. This could lead to systematic bias and result in overlooking a class of possible cause-and-consequence relationships and future outcomes that may be relevant to the advising mission.

Additional Legal and Multinational Obstacles to Outsourcing Strategic Management of Advisors' Intellectual Capital

At this point we examine two general types of obstacles that limit the ability of (traditional) intelligence organizations to support the sociopolitical analysis needs of a ministerial-level security sector reform advising mission. The first type occurs out of concern for compromising counterpart relationships, due to the suspicion associated with advisors interacting with intelligence personnel. If there appears to be regular consultation with known intelligence personnel, advisors can experience the advising mission hazard of becoming de facto human intelligence collection assets. There also exists a pervasive concern that information shared outside of the advising mission could end up in open channels (e.g., Wikileaks).

The second type occurs because of the unique needs of a ministerial-level advisor. Even if intelligence organizations could legally support the advising mission, the authors have discussed above how and why ministerial-level advisors would be their most difficult customers to satisfy. Intelligence organizations' resource and access limitations as well as the threat emphasis severely limit their abilities to support ministerial-level advisors. In Afghanistan, operational- and headquarters-level military intelligence resources are limited and judiciously applied only to supporting the ISAF mandate for security assistance in countering the insurgency. The Priority Information Requirements (PIRs)[768] they respond to involve a tightly bounded definition of the threat–where it is, what it has and what it can do. Since ANA-DEV was focused on building capability and capacity in the Afghan security forces, and not concerned with the security threat directly, operational military intelligence was not positioned to address ANA DEV's needs.

Legal and multinational constraints on the campaign create additional obstacles to intelligence organizations supporting the sociopolitical needs of ministerial-level advising missions.

- Unique national information handling caveats and national intelligence classifications hamper multinational actions and/or information sharing. The simple existence of the U.S. Combined Security Transition Command-Afghanistan (CSTC-A), a nationally exclusive organizational element initially separate from the NATO Training Mission-Afghanistan, operates outside of the alliance to control national contributions and participation in the operation.[769] With respect to intelligence classification, because of the ambiguous multilateral information-security environment, policies to clarify what information elements need protection could not be issued. ISAF lacked authority to impose a unified and coherent security classification policy because the multilateral environment included both national voluntary and bilateral, Afghan government-accepted troop contributions that fell outside of a unified NATO umbrella.

- Some Afghan counterparts have spent time in the United States, become affiliated with U.S. corporations, and even married U.S. citizens. These Afghans therefore fall in the category of "U.S. Persons" with legal protections against U.S. intelligence collection.

- Most contractor advisors in Afghanistan are employed under Statements of Work (SOWs) that prevent them from providing advising-derived information to intelligence organizations.

- Most critically, Afghanistan is a sovereign ally and NATO Training Mission-Afghanistan's mandate is subject to annual renewal by the U.N. Security Council. The U.S. Intelligence Community is legally restricted in how it can collaborate with the sovereign government of an allied nation, and ISAF has limited roles, authorities, and responsibilities under United Nations Security Council mandates.

In the advising domain, ANA-DEV was functionally a task force both in structure and because of the commander's having Critical Information Requirements (CCIRs). Given the advising mission's unique information analysis, knowledge management, and advising relationship protection and

preservation needs, most of those CCIRs could not be met from outside ANA-DEV if all alliance legal requirements were to be upheld.

Solving the Problem

ANA-DEV leadership was keenly aware of the loss of advisor intellectual capital upon redeployment and moved to stem this loss of understanding and influence. The ANA-DEV command approved an initial proposal allowing the authors to work as a team to create an internal capability that would interview senior advisors to capture their insights and experiences, develop and refine this information with historical and cultural context, and then educate the advisors' successors. This team served as an organic capability for capturing, analyzing, and holding the mission's intellectual capital by creating "enhanced continuity" of advisor's insights and influence. By fulfilling all four characteristics of strategic management of intellectual capital, this internal capability would facilitate the advising mission's becoming a learning organization. The team was also tasked with developing standard operating procedures for managing, retaining and protecting advisor information of a sensitive nature for the advising relationship. In short order, this advisor-staffed research and analysis team would carry out additional duties, including developing factional studies and orders of battle for the MoD and general staff, creating "one-shot" research projects at leadership and individual advisor request as well as initiating a quarterly comprehensive survey of advisors' insights into their counterparts' attitudes toward security sector reform projects and initiatives.

ANA-DEV did not view having an organic research and analysis capability as stepping uninvited into the intelligence playing field. Far from it, ANA-DEV as an operational advising mission was centrally concerned with avoiding any potential threat to the counterpart relationships. An organic research and analysis capability staffed by advisors under ANA-DEV's operational control and with no reporting requirements to parent organizations mitigated all risk associated with an advising mission engaging with intelligence in a Smart Power environment for purposes other than force protection.

To meet ANA-DEV's needs, team members needed to be highly motivated volunteers from within ANA-DEV who enjoyed strong rapport with and trust of fellow advisors. They needed to have deep knowledge of Afghan culture,

politics, history, and language skills. Most importantly, team members needed to bring relevant analytical skills, knowledge of social science methods, and applied research experience to bear in analyzing and understanding each day's novel developments.

The concept required each member to challenge conventional wisdom, separate facts from opinions and assumptions, and continuously pursue new information and knowledge. All team members needed to have the same degree of access to officially protected information, and be highly knowledgeable of and strictly observant of relevant ethics codes and legal restrictions. After a month of surveying best practices, crafting standard operating procedures and interview protocols and instruments, and designing foundational products that could be regularly updated, ANA-DEV established the first Sociopolitical Network and Behavioral Analysis Team (SNBAT).

The SNBAT was established as a dedicated, organic element within ANA-DEV and under the direct control of the ANA-DEV commander or his deputy. This direct control included requiring written authorization by the ANA-DEV commander for the distribution of any analysis products. The commander needed the SNBAT to be flexible and responsive to CCIR's, which reflected the dynamic and highly fluid advising environment. SNBAT personnel actively participated in daily ANA-DEV advisor meetings and huddles not only as MoD advisors but also to anticipate upcoming and changing information needs. Since these meetings were typically closed to all but ANA-DEV advisors, the dedicated, organic relationship was vital to advisor acceptance of and cooperation with the SNBAT.

Although ANA-DEV's SNBAT was the first of its kind for ministerial advising, it was designed to address knowledge gaps based on best practices of prior efforts. While the SNBAT concept is embedded in an advising mission's need for unique analysis support, the authors found the best models for balancing flexibility and commander control in how Analysis Control Teams (ACTs), "Augmented Military Transition Teams" (MiTTs) in Iraq, and Company Intelligence Support Teams (CoISTs) were organized. The small, focused ACT could and did provide value in Iraq when brigade commanders directed them to focus where the "fog of war" was a potential hazard for the operation. The "Augmented MiTTs" in Iraq were able to fill information gaps after receiving

autonomy from their parent brigades. CoISTs are another example of using personnel organic to the operational mission to address knowledge gaps.[770]

Staffing the ANA-DEV SNBAT

ANA-DEV initially staffed the team by capitalizing on some of its Afghanistan-Pakistan Hands (APH) advisors. The U.S. Joint Chiefs of Staff Hands program has developed a cadre of civilian and military personnel with understanding of Dari or Pashto through four months of immersive language instruction, together with familiarization with "culture, religion, tribal dynamics, central and provincial government structures and processes, Afghan security structures and processes, among other subject matter expertise."[771] Later, when a founding team member redeployed, that seat was filled by a Ministry of Defence Advisor (MoDA). The U.S. Defense Security Cooperation Agency's MoDA program "is designed to forge long-term relationships that strengthen a partner state's defense ministry. The program matches senior Department of Defense civilians with partner-identified requirements…. While deployed, the advisors exchange expertise with foreign counterparts in similar defense specialties."[772] MoDA training includes a comprehensive seven-week course that covers advisor training, Afghanistan cultural awareness and country familiarization, as well as Dari language instruction.[773]

Staffing the SNBAT with "Hands" and MoDA advisors made it feasible to keep the SNBAT under the ANA-DEV commander's authority. In theater, "Hands" and MoDAs are "op-conned," in that they are placed under the operational control of the commands to which they are assigned. The SNBAT team's organic, op-conned status contributed to gaining trust and support from ANA development advisors and leaders, since no conflict of interest could arise with respect to a need to produce, share, or archive products or reports for promotion in or support of other chains of command.

A key SNBAT activity was interviewing ANA-DEV advisors to capture their insights and benefits of experience. To be fully effective, in addition to capturing sociopolitical insights, the interview had to be an exchange of experiences and ideas that stimulated the guest advisor to recall and share valuable insights, share moments of cross-cultural understandings and misunderstandings, and to think through new interactional techniques that contributed to or would have improved rapport with their host-nation counterpart. To

ensure the interviews captured a two-way flow of information, SNBAT personnel had to be skilled in Afghan sociopolitical knowledge and ministerial advising and able to put fellow advisors at ease during the interviews.

ANA-DEV Knowledge Management Data Handling

Knowledge management was a core SNBAT responsibility. Although advisors' data are not typically threat relevant, they are potentially highly sensitive with regard to developing advising relationships. The team secured all data to ensure commander's oversight, and exceed established tenant unit requirements in a manner consistent with the ethical obligation to maximize advisor safety. SNBAT regarded advisors as inherently "owning" their information and treated them as having originator control over their data, with that control to be "inherited" by their successors. This effectively placed advisors in control of the extent to which their data would be used in SNBAT products. After derivative products were produced, only the commander could designate their distribution and use. A cross-functional knowledge of theater data repositories facilitated the distribution of commander-directed release of SNBAT products.

SNBAT knowledge management requires appreciation for librarianship. Advisors will often exchange books and articles they find helpful during their tours. The SNBAT office became the site of the advisors' library, which SNBAT members expanded with purchases of locally published books, particularly history books. This feature grew in importance as the team learned more about different ethnic groups' accounts of historical events, some of which differed sharply with conventional wisdom and official accounts. Also, understanding the complexities of Afghan political and social history in the pivotal 1960s and 1970s became crucial for understanding the formative events and social networks forged during the early careers of older Afghan MoD counterparts.

ANA-DEV SNBAT Products

The primary rationale for creating a SNBAT is to maintain advisor continuity—to mitigate loss of the tactical social advantages, insights, and knowledge the departing advisor has developed over the course of an advising year. To produce the first advisor continuity brief required designing an interview instrument extensive in both scope and depth that would (a) capture the full scope of the advisor's knowledge of and relationship with their counterpart and (b)

capture the advisor's insights into their counterpart's relationships within the MoD, within the Afghan government, and within wider Afghan society.

The interview instrument was extensive, with over 38 pages of questions that typically took 5-6 hours. The length was necessary in order to capture the full range of the year's advising experience. SNBAT interviewers initially thought advisors would resist and refuse to sit for the interview because of its length. However, despite some initial refusals, the SNBAT met its goal of successfully and fully interviewing most departing senior advisors after the first month of team operation. The breakthrough was the spread by word-of-mouth that the interview, though long, did a good job of capturing advisor experiences over the course of their advising year. The authors also found that SNBAT messaging allayed advisor concerns about being judged. The SNBAT never drew conclusions about an advising relationship on the grounds that each advising relationship was unique and an advising relationship's success is at least equally in the hands of the counterpart. After a successful initial trial period, ANA-DEV leadership made sitting for the SNBAT advisor continuity interview mandatory for redeploying advisors.

The SNBAT interview instrument had four sections: Evaluation of the Counterpart, Counterpart Interactions with Others, Counterpart Personal Life History, and Counterpart's Office Location, Layout, Schedule, and Tempo. Within each section there were clusters of similar questions designed to help prompt advisor recall on a variety of subtopics.

Two additional features of the instrument were particularly useful: a descriptive personality inventory, and descriptive means for an advisor to identify their counterpart's cognitive/learning skill levels. These provided advisors with a standard lexicon for describing their counterparts. The authors inserted these features because information about counterpart personality traits and learning levels are very important for new advisors. Departing advisors' answers to these questions established a baseline so future advisors could have a basis for comparison if there was concern about the counterpart's cognitive or emotional state.

The SNBAT also leveraged social network analysis. Advising missions continually grow, change, and transition. Advised ministry counterparts may be newly appointed, promoted, retired, and/or laterally moved. Ideally, friction

and failure points should be identified before a partnered organization is stressed to absorb and implement institutional change required by the advising organization. With a social network analysis capability, the commander can identify relationships that may facilitate or strain the advising effort and facilitate or hinder the capacity for change within the partnered organization.

This capability was the backbone for a second cumulative SNBAT product. The SNBAT produced an "order of battle" distinguished by identification and overlays of factions and informal social groups within the Ministry of Defense and general staff. The driving rationale for this product was recognition that informal influence often mattered as much as formal authority during the interim flux period of security sector reform when the advised security institution's professional standards are being identified, codified, and propagated. Advisors were keenly aware of these different types of power[774] and how influence could trump authority to the detriment of military professionalization. The SNBAT drew from advisors' pooled insights to identify factional and social group sources of influence beyond broad ethnic membership categories. Both the advisor continuity brief and the order of battle required several months of intellectual capital accumulation before they started to provide a bird's eye view of patterns and relationships.

A third SNBAT product initiative was a quarterly survey of advisors. This product was designed to indirectly capture attitudes and opinions within the MoD about advising mission policy initiatives and progress toward meeting those initiatives. The quarterly survey's questionnaire was a mix of open- and close-ended questions that probed MoD attitudes toward current mission objectives and allowed advisors to note their counterparts' emergent concerns. This survey differed from the Advisor Continuity brief by having a primary focus on the contemporary (with only limited historical content) and by being a total "snapshot" capture of attitudes in a relatively short period of time. ANA-DEV leadership and advisors thus had their first comprehensive understanding of attitudes and opinions in the MoD about current initiatives and emergent concerns analyzed within a context of sociopolitical factors and cleavages.

Over time, the SNBAT started to receive requests for "one-shot studies." The SNBAT fielded requests for information from advisors on many topics, including gender relations, traditional governance and dispute resolution, social

factions, civil society, social aspects of health and medical care, general history, religious social organization, differences in attitudes between Kabul and other areas, and others.

The SNBAT Life Cycle and Future Applicability of the SNBAT Concept

Security sector advising missions are not permanent. All advising missions seek to, in the words of a senior NTM-A leader, "work themselves out of a job." As advisors work toward successfully concluding their mission, transitions and personnel changes will take place, including changes to organic capabilities such as the SNBAT.

Near the close of 2011, NTM-A reorganized some of its subordinate commands, including ANA-DEV, in light of the new goal of transitioning security functions to Afghanistan National Security Forces by 2013. A few months later, ANA-DEV as a subordinate command ended its separate existence and merged with another. The ANA-DEV SNBAT, being organic to that command, ceased operating. The winding down of the ANA-DEV SNBAT was natural and rational: as an organic, dedicated capability to a command, when that command is reorganized or drawn down, the SNBAT follows those same organizational fortunes. Had the SNBAT remained in operation apart from the advising mission and under a rationale different from managing that mission's intellectual capital, it would have veered improperly into the intelligence realm. As ANA DEV wound down, the ANA-DEV SNBAT's entire organizational life-cycle went through a successful proof-of-concept. By having done so, the SNBAT concept in its life-cycle entirety can be applied to other advising missions in the future.

To that end, what can future advising missions, outside of NATO's Afghanistan campaign, that wish to preserve and utilize their advisors' intellectual capital, learn from ANA-DEV and its SNBAT?

- All security sector advising missions are smart power initiatives. Smart power not only increases the need for sociopolitical understanding, but also the scope and levels of needed sociopolitical understanding.

- Sociopolitical understanding of the advising environment is not simply adding individual advisor insights; advisor insights must be relationally combined into a coherent, corporate body of intellectual capital.

- Intellectual capital is not produced by a few sociopolitically astute advisors; rather, intellectual capital requires contributions from every person within the advising organization.

- Advising missions must be proactive about compiling, analyzing, fusing and retaining intellectual capital. If advising missions do nothing, advisor replacement cycles will cause time-driven cyclic exodus of intellectual capital that requires a substantial amount of time and interaction to rebuild–if it can be rebuilt at all. When organizations are proactive about their intellectual capital, they become learning organizations.

- Strategic management of intellectual capital is an internal, organic organizational activity because intellectual capital is the critical component for becoming a learning organization. An advising mission that outsources its intellectual capital management to outside organizations foregoes becoming a learning organization.

- Strategic management of an advising mission's intellectual capital by outside organizations (especially by an intelligence organization) creates hazards including potential compromise of counterpart relationships, advisor hesitance to contribute to intellectual capital, counterparts who may be U.S. persons with legal protections against U.S. intelligence collection, and sovereignty issues.

- Strategic management of an advising mission's intellectual capital by outside organizations is doomed to failure in meeting the advising mission's sociopolitical needs. Advising missions' sociopolitical understanding is embedded in policy analysis and knowledge of the security institution's capacity building. The expert source for these twin bodies of knowledge is the advising mission itself, which makes an outside analyst more dependent on the advising mission that the advising mission is dependent on the outside analyst.

- SNBAT members need to have strong rapport with, and be trusted by the advisor corps. All team members must have the same degree of access

to officially protected information, and, regardless of their position on the team, equally contribute to analysis. Each team member must be knowledgeable about the host-nation's history, culture, politics, and society and have facility in a language. Additionally, team members must bring diverse advanced skills to the team and team members must recognize and respect those skills.

- SNBAT team members need to be under the operational control of the advising mission commander *and no other*. The commander's direct control must include control over the distribution of any analysis products.

- Advisors maintain control over their data, with that control to be inherited by their successors. The SNBAT holds advisors' data in order to ensure its handover from the originating advisor to the successor advisor.

Conclusion: The SNBAT's Indirect, Residual Benefits from an Intelligence Manager's Perspective

Throughout this essay the authors have analyzed intellectual capital needs, problems, and the SNBAT solution from the perspective of commanders leading advising missions in complex smart power environments. The triad of increased needs for sociopolitical understanding, discretion in operational mission direct engagement with host nations for partnering, and organic strategic management of mission intellectual capital is not unique to advising missions. They are needs for any operational mission partnering with a host nation and will intensify in multinational campaign contexts. These are evolving consequences of smart power, and just as the rise of smart power has consequences for the operational side of security sector reform, it will also have consequences for the intelligence side.

However, the authors' explanation of why an advising mission's SNBAT activities must remain apart and separate from traditional intelligence organizations does not mean that SNBAT activities existed in opposition to intelligence organizations or to their missions. Autonomy does not equate with opposition and indirect, residual benefits can accrue to intelligence. However, for that to happen will require that intelligence refrain from viewing SNBAT initiatives as a resource to absorb, subsume, or task. This will not be a challenge, as parallels

exist in which the U.S. Intelligence Community has indirectly, residually benefited from maintaining the autonomy and independence of non-intelligence research and analysis efforts.

With the increased value the Intelligence Community places on cultural analysis,[775] it is becoming more difficult to distinguish the analytical products of several intelligence analysis specializations from academic publications or the development aid measurement and evaluation specialist's baseline field studies. The waters become even more muddied when one considers that each profession's products involve protection of the information analyzed, though in different ways. The intelligence analyst classifies the product within a system that tightly regulates who will have access. The academic is legally and ethically obligated to protect the identity of their collaborating research sources under U.S. federal human subject protection laws. The development measurement and evaluation specialist is required to carry out research under the principle of "do no harm." However similar the products and imperatives to protect data may be, it is the organization within which and the audience/customer for which the analysis is conducted that determines whether the research and analysis is an intelligence product. The Intelligence Community does benefit from openly and publicly available academic and development baseline studies. Intelligence managers recognize that attempting to absorb, subsume, or task the university academic or the development organization specialist would imperil those individuals' ability to carry out research and contribute to the public knowledge from which the Intelligence Community also benefits.

Although the indirect, residual benefits from a SNBAT initiative are different, seeking to absorb, subsume, or task an operational mission's SNBAT would likewise imperil its ability to carry out research and analysis to produce those benefits. What are those indirect, residual benefits to the Intelligence Community?

- The first and foremost indirect benefit is fewer advising mission requests for information. An advising mission's SNBAT initiative allows intelligence to focus on threat (its traditional strength). A SNBAT capability does this by focusing on directly empowering advisors with knowledge, not on building a knowledge base they may not be able to directly access.

- A second benefit, particularly for the Intelligence Community's increasing focus on cultural analysis, is increasing the numbers of those with specialized sociopolitical subject matter expertise. SNBATs empower advisors by increasing the scope and breadth of their knowledge about the relationships between the advised ministry, national government, and subnational government/commands. While advisors are "correctors, not collectors" these enhanced insights into individual and relational social, political, and behavioral trends and tendencies are in a category of foundational knowledge comparable to the published academic insights open- and all-source intelligence analysts find useful and seek out.

- A third benefit stems from security sector advising efforts to build the partner nation's intelligence capabilities and capacities. This effort requires advisor staffing by individuals with intelligence backgrounds who are and remain under the operational command of the advising mission. The operational command requirement, for the safety of the advising mission, necessarily suspends that advisor's relationship with any sending intelligence organization for the duration of the deployment. However, the indirect benefits of foundational knowledge insights that such an advisor can gain and return with upon redeployment are far different from those that accrue to simply being "deployed forward" as a sending organization's analysis asset. True mentoring and relationship building (as opposed to simply liaising) allows the individual unparalleled access to social, political, and cultural ontologies and ethnographic knowledge. This is an invaluable human capital investment in the analyst and one made possible by the advising mission's strategic management of its *own* intellectual capital.

- A fourth benefit results from the SNBAT solution for protecting advisors' sensitive information. Multilateral smart power environments yield multinational organizations that often move forward prior to establishing unifying intelligence policies and guidance that single-nation operations take for granted. With a SNBAT, advisor information can be protected from undesired disclosure without defaulting to single-nation solutions inapplicable to an organization governed by international mandates.

Other indirect, residual benefits will undoubtedly occur to the reader. However, any of those benefits will accrue only through the autonomy of the advising mission's SNBAT capability.

The authors have explained how smart power environments shape advising missions, their need for sociopolitical understanding, and constraints in meeting those needs. As smart power represents an evolutionary step in U.S. national security and foreign policy, so must its associated operational and intelligence efforts adapt. The ANA-DEV SNBAT is an illustration of how the authors' successors may adapt organizationally to smart power environments.

About the Authors

Colonel William S. Brei advised at the Afghan Ministry of Defense while serving in the Afghanistan-Pakistan Hands Program. He was the first and founding ANA-DEV SNBAT chief. During earlier deployments he served at Bagram Air Base in 2002 and as the director of the Mazar-e Sharif International Airport in 2005. He retired from the U.S. Air Force in 2012 after a 28-year career. *WSBrei@yahoo.com*

Nathalie J. Frensley, Ph.D. advised at the Afghan Ministry of Defense while serving in the Afghanistan-Pakistan Hands Program. She was the first and founding SNBAT research director and second SNBAT chief. Previously, she was an associate research scientist at the Institute for Advanced Technology, the University of Texas at Austin. Corresponding Author. *NJFrensley@gmail.com.*

Major Killaurin O. Roberts advised at the Afghan Ministry of Defense while serving in the Afghanistan-Pakistan Hands Program. He was the first and founding SNBAT deputy for assessments. Previously, he served NATO as an ISAF theater fusion chief and served U.S. Forces as an operational intelligence mentor during both the Iraq and Afghanistan surges. *Killaurin.Roberts@us.army.mil.*

Conclusion

Carolina Sancho Hirane

This book is the third in a series that began with *Professionalization of Intelligence in the Americas*. The latter, published in 2004, addresses the phenomenon of government intelligence from the perspective of public servants who are engaged in the professionalization of the function throughout the Americas. The work identifies the challenges facing professional development efforts, a chief concern of intelligence services at the time, and traces the paths chosen by various countries to arrive at that stage of development.

The second book in the series, *Democratization of the Intelligence Function*, from 2009, examines how the reinstatement of democratic political systems in the region has affected the intelligence services. At the same time, the book addresses the effect of distinctive strategic intelligence cultures on the development of intelligence institutions.

This book goes beyond the two earlier works in bringing a particular focus to the challenges that confront intelligence services as they carry out their responsibilities in an environment strongly influenced by forces of globalization. Threats to national and public security in each country have become increasingly similar to those of other countries of the hemisphere. Notwithstanding the wide variety of political, social, cultural, administrative and historical contexts represented in the region, intelligence services expect to operate transparently and within legal boundaries as they develop capabilities, expertise, and leadership consonant with their societal role.

The question that has guided this academic work is "How can we address the challenges to intelligence management that arise from various quarters and at various levels?" The answer emerges from essays presented in four sections. Each set of essays explores several aspects of the challenges found at each level of intelligence management, beginning with societal and institutional oversight of intelligence, then addressing executive branch management options, continuing with intelligence system or community management of privacy and security issues, and concluding with professional self-management through intelligence integration opportunities.

The first section explores the legal framework within which intelligence services operate. More judicial regulation, a part of the democratic transition in the region, has increased external control of intelligence services. In addition, the region at large has passed through a learning process marked by intelligence scandals and unprofessional practices. Congressional or parliamentary oversight has only a brief history, but has grown through trial and error. It is clear that further improvement in oversight is needed, especially if one compares intelligence oversight to the more rigorous oversight exerted in other areas of public administration.

One of the defining characteristics of intelligence is its operational secrecy. Secrecy allows intelligence to carry out its societal role, to meet its responsibilities and to accomplish its missions. However, secrecy runs squarely in opposition to the principle of transparency in a democratic political system where government acts on behalf of citizens. This is where one finds an unmistakable tension between efficiency in the management of a public service on the one hand, and that service's legitimacy and transparency on the other hand. In this situation the overall quality of a democracy hangs in the balance. Adequate oversight would, under conditions of non-disclosure, allow non-intelligence public officials access to intelligence information, intelligence sources and methods, and knowledge of intelligence actions. Effective oversight stimulates and promotes responsible management within the intelligence services, so that they may make appropriate use of the decisionmaking latitude granted to them by the legislature. The countries of the hemisphere continue to make slow progress in the realm of oversight as, mainly through trial and error, they develop viable institutions for intelligence management.

The greater autonomy granted to the intelligence services in comparison with other public services, especially in terms of their being able to operate in secrecy, emphasizes the importance of promoting and strengthening ethical behavior among intelligence employees. The difficulty of finding real-world examples to illustrate workplace ethics has been alleviated by the existence of several exemplary, popular films. The public at large has the opportunity to examine these productions and explore the opposing values that intelligence practitioners regularly encounter, among them questions of freedom, security, privacy and respect for human rights. The films often leave these questions without full resolution, therefore inviting viewers, whether private citizens or

intelligence officials, to engage in a discussion of ethical practice. In the long view, such discussion can bring concrete answers to ethical challenges.

This practical approach to intelligence ethics emerges as one part of the answer to the book's central question of how we might address the challenges that confront intelligence management. An ethical approach to intelligence practice can be reinforced in several ways. One option is to develop an ethical code of conduct, something that has not yet been accomplished in the region. Meanwhile, the intelligence services themselves, supported by suitable external oversight, can create incentives for the appropriate use of the autonomy and institutional secrecy they have been entrusted to employ.

Section two explores the role of the executive branch in managing the production and use of strategic intelligence. Although considerable prejudice and confusion surround these issues, there is consensus about what strategic intelligence should be able to accomplish. One author argues that economic phenomena deserve greater intelligence attention at the strategic level. Another author explains the relationship between intelligence and the budgeting process, an area too often ignored at the national level of executive decision-making. Directives issued from this level, for example, typically make little or no mention of the resource needs of the intelligence services. Under these circumstances, it falls to intelligence officials themselves to explain clearly and precisely the relationship of financial resources to information requirements formulated at the national political level, and to specify how those requirements translate into particular intelligence resources.

The rise of international cooperation among intelligence services has become a particularly controversial aspect of executive branch intelligence management. Elected officials as well as the intelligence services themselves often view such cooperation with suspicion. Cooperation seems to place secrecy at risk and exposes an intelligence service's vulnerabilities. Critics also feel that differences among countries are greater than their similarities, and that the importance of those areas in which countries compete prohibits them from developing a relationship built on similar interests. However, the increasing proliferation of transnational threats to security, as well as government statements recognizing common security threats, allow a more hopeful view of future progress toward intelligence cooperation in South America. This tendency is reinforced by the fact that each country of the region does have

experience in strategic, military and police intelligence, as well as a demonstrated ability to cooperate multilaterally in each of these areas. A remaining challenge exists in the lack of intelligence cooperation under the auspices of UNASUR, although such cooperation already takes place in other multilateral organizations in the region, and may be exported to UNASUR itself.

The third section of the book explores how national systems or communities manage the tension between privacy and security in the course of daily intelligence activities. In principle, personal or sensitive information about citizens is private, and can be accessed only by authorized and justified exception to this principle. In the context of intelligence work, and wherever its activity is regulated by recently enacted laws, procedures have been developed to guide intelligence access to information about individuals. Typically, access depends on prior approval by a government office external to the intelligence services. However, these procedures have not always worked as expected; that is, as a reliable counterweight to the autonomy of those services—to keep them from accessing private information about citizens and making unethical use of the information.

Existing information and communications technology, together with the widespread use of social communications media, make immense quantities of information available to the intelligence services, leaving in the past the problem of not having enough information, but introducing the challenge of processing the information—evaluating it, classifying it, and mainly, analyzing it. On the other hand, legitimate questions remain not only about intelligence access to this information, but also about how long it may be retained. In this new world, the classical principles that have guided acquisition of information about private citizens have been overturned, in the sense that information formerly was obtained on an exceptional basis, for a defined period, and with evident justification (that is, probable cause). The resolution of this problem now appears to require international consensus because the outcome of the debate will have consequences for most countries whose intelligence services are regulated by laws.

From a national perspective, the requirement to devote greater attention to the development of the state intelligence function raises the question of which agencies should become members of an intelligence system or community. The need to define and create a framework for criminal and prison

intelligence, for example, calls for a review of what each potential element of a national system or community may contribute to the collective effort. Managers need to determine how strategic, police, and military capabilities may best relate to each other within the public security and national security contexts. Best practices and lessons learned about the growth of intelligence communities in the Americas and Europe need to be analyzed and modified as needed for application in South America.

In addition, the issue of ensuring adequate interagency cooperation and coordination within an intelligence system or community requires a review of national legislation and agency accountability. The review can help ensure that cooperation and coordination are carried out in the intended fashion and for the intended purposes. At stake in this review is a determination of the very legitimacy and legality of these cooperative practices, together with the prospect of either gaining or losing international respectability and a positive public image as a result of having or not having in place an effective and efficient intelligence system.

The last section of the book deals with three facets of integration management carried out by the intelligence services themselves. First, internal intelligence education serves an integrative function by ensuring that practitioners understand the operational role of each of branch of government, and gain familiarity with the contribution of all government organizations that collect and analyze information. Externally, intelligence professionals in the region have access to strategic studies or intelligence studies programs in universities. Internal intelligence education can accommodate classified material, but external education holds greater value for professional development when the comprehension of more general and multidisciplinary subjects requires debate and critical thinking. A few private institutions across the region have developed seminars capable of offering the detailed, expert coverage of sensitive topics suitable for specialists, but these programs are not exclusively for government intelligence practitioners.

A second facet of intelligence integration involves the management of information and communications technology, important because this technology rules a good part of our daily personal regimen. Sometimes described as the fifth dimension of warfare but in reality much more than that, cyberspace is where people conduct much of their daily lives. It is also where national

boundaries are meaningless and anyone can operate essentially without limitation. This environment challenges those who intend to administer it or to manage its security issues. The nature of cyberspace gives full play to concepts like "glocal" and "intermestic," as governments or private interests try to counter cyberattacks or the unlawful use of online information. An action taken on one side of the world using a server located there can effect changes in or even be lethal to a system located on the other side of the earth (a prime example being the control of nuclear reactors). Similarly, an attack on a web page may originate in any place in the world and bring serious consequences to local residents who wish to make use of the page.

The huge quantities of available information require a review of how it may be accessed, the conditions under which it is accessible, and how that access may be controlled. The issues of information security and access to information in cyberspace for intelligence purposes require a suitable adjustment to current management deficiencies. One solution may lie in developing a legal framework to regulate intelligence access in a way that prevents abuse. Political legitimacy for intelligence access to information depends on the outcome of public debate.

Another aspect of information integration involves the multilateral environment of political-military advising missions. In the case of U.S. advisors in Afghanistan, a field experiment illustrates how innovation in information integration can replace the traditional intelligence apparatus. Integrated information management can play a role similar to that of intelligence where traditional, unilateral intelligence capabilities remain unwelcome or unlawful.

Democratic political systems and globalization make intelligence management in the hemisphere a complex task. Complexity arises from the variety of issues to be considered, the variety of actors involved, and the sensitive nature of the subject itself. No one person can bring about effective management of this governmental function. The task requires multidisciplinary effort. This book has sought to contribute to that undertaking.

References

1 Russell G. Swenson and Susana C. Lemozy, coords., *Intelligence Professionalism in the Americas* (Washington, DC: Joint Military Intelligence College, 2004), *http://www.ni-u.edu/ni_press/pdf/Intelligence_Professionalism_in_the_Americas.pdf*.

2 Russell G. Swenson and Susana C. Lemozy, coords., *Democratization of Intelligence* (English excerpts) and *Democratización de la Función de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estratégica* (Washington, DC: National Defense Intelligence College, 2009), *http://www.ni-u.edu/ni_press/pdf/Democratization_of_Intelligence.pdf* and *http://www.niu.edu/ni_press/pdf/Democratización_de_la_Función_de_Intpligencia.pdf*, respectively.

3 Guillermo Valdes Castellanos, Director of the Center for National Intelligence and Security (CISEN) from 2007 to 2011, in *CISEN: 20 Años de Historia—Testimonios (México:* CISEN, 2009), p. 12. CISEN is the civilian intelligence agency of Mexico.

4 Castellanos, *ibid*, p. 13.

5 Fredy Rivera Velez and Katalina Barreiro Santana, "Inteligencia estratégica: algo más que curiosidad mediática o (in)discrecionalidad política," in Fredy Rivera Velez, coord., *Inteligencia estratégica y Prospectiva* (Quito: FLACSO Ecuador & National Secretary of Intelligence, 2011), p. 37.

6 See the brief description of SENSIPAM on the main page of the System for the Protection of the Amazon (SIPAM) at *http://www.sipam.gov.br/*. Accessed 12 August 2012.

7 See, for example, the definition of "national intelligence" in U.S. Public Law 108—458, Intelligence Reform and Terrorism Prevention Act of 2004, section 1012, *http://www.nctc.gov/docs/pl108_458.pdf*. Accessed 14 August 2012.

8 J. Edward Conway, "Analysis in Combat: The Deployed Threat Finance Analyst," *Small Wars Journal* (July 2012), *http://smallwarsjournal.com/jrnl/art/analysis-in-combat-the-deployed-threat-finance-analyst*. Accessed 30 July 2012.

9 See Federation of American Scientists, Intelligence Resource Program, at *http://www.fas.org/irp/world/index.html.*

10 Richard Helms, *A Look over My Shoulder: A Life in the Central Intelligence Agency* (New York: Random House, 2003), pp. 3-13.

11 Clifford Krauss, "Tapes Spy Chief Left Behind Scandalize Peru," *New York Times*, 3 February 2001, *http://www.nytimes.com/2001/02/03/world/tapes-spy-chief-left-behind-scandalize-peru.html?pagewanted=all&src=pm*. Accessed 1 August 2012.

12 Florina Cristiana Matei and Thomas C. Bruneau, "Policymakers and Intelligence Reform in the New Democracies," *International Journal of Intelligence and CounterIntelligence* 24, no. 4 (Winter 2011/2012), pp. 656-691, and Maria do Ceu Pinto, "Portugal's Intelligence Evolution in the Post-9-11 World," *International Journal of Intelligence and CounterIntelligence* 25, no. 1 (Spring 2012), pp. 160-177. Matei and Bruneau also cover Poland, Romania, and Russia in their essay.

13 Gregory Weeks, "A Preference for Deference: Reforming the Military's Intelligence Role in Argentina, Chile and Peru," *Third World Quarterly* 29, no. 1 (2008), pp. 49-58. The author finds that of these three countries, only Argentina has placed military intelligence activities under civilian oversight.

14 Matei and Bruneau, *op. cit.*, p. 682.

15 Ceu Pinto, *op. cit.*, pp. 165-167.

16 In the United States, for example, Executive Order 12333 (1981), in its part 2, spells out prohibitions on collection activity, *http://www.archives.gov/federal-register/codification/executive-order/12333.html*. In addition, individual parts of the Intelligence Community may have additional guidelines. For example, *Procedures governing the activities of Department of Defense intelligence components that affect United States persons, December 1982, http://atsdio.defense.gov/documents/52401-R.html*. Documents accessed 2 August 2012.

17 Inter-American Court of Human Rights, Demanda en el caso de Humberto Antonio Palamara Iribarne (Case 11,571) against the Republic de Chile, 13 April 2004.

18 Richard J. Aldrich, "Beyond the Vigilant State: Globalisation and Intelligence," *Review of International Studies* 35 (2009), p. 900.

19 Richard J. Aldrich, *ibid.*, p. 898. For an appreciation of the importance of informal information and intelligence collaboration among police forces, see Michael D. Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Intelligence University Press, 2010), ni-u.edu/ni_press/pdf/The_Blue_Planet.pdf.

20 Aldrich, *ibid.*, p. 900.

21 Claudio Fuentes, "Political Dimensions of Security Transformation in Latin America," *Institute of Development Studies Bulletin* 40, no. 2 (March 2009).

22 For example, see the anonymous Intelligence Community source for James Bamford's, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), p. 1.

23 See Gary Ross, *Who Watches the Watchmen?—The Conflict between National Security and Freedom of the Press* (Washington, DC: National Intelligence University Press, 2011), *http://ni-u.edu/ni_press/pdf/Who_Watches_the_Watchmen.pdf*. Accessed 11 August 2012.

24 Two interesting examples are: Jesus Emilio Garcia Acosta, *El Ave del Pantano: Una Novela sobre la Inteligencia Estatal—el Segundo arte más antiguo de la humanidad y el primero de los dioses* (Bogotá: Editorial la Serpiente Emplumada, 2007) and Bravo Leon, *El Espía Frances: Crimen, Corrupción y Tráfico de armas en Chile* (Santiago: Origo Ediciones, 2011).

25 See, for example, the results of a study by political scientist Elizabeth A. Bloodgood, "What Do Decision-Makers Know?: The Sources and Evaluation of Information in Foreign Policy," paper presented originally at the annual meeting of the International Studies Association, February 2003, in Portland, Oregon, *http://www.allacademic.com//meta/p_mla_apa_research_citation/0/6/4/5/6/pages64568/p64568-1.php*. Accessed 12 August 2012.

26 Ohad Leslau, "The Effect of Intelligence on the Decisionmaking Process," *International Journal of Intelligence and CounterIntelligence* 23, no. 3 (Autumn 2010), pp. 426-448.

27 Stevyn D. Gibson, "Future Roles of the UK Intelligence System," *Review of International Studies* 35 (2009), pp. 920-921.

28 Gibson, *ibid*, p. 923.

29 See Richard J. Aldrich, *op. cit.*, pp. 891, 896-898. The author points out that today, because of the close linkage of intelligence and operations, "secret services are doing less analysis and estimating and more 'fixing, enforcing and disrupting.'" In this light, U.S. intelligence's "rendition" of operatives to Guantanamo was as much about disrupting al-Qaida's core structure as it was to extract information from them.

30 Robert M. Gates, "An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House," *Washington Quarterly* 12, no. 1 (Winter 1989): 35-44.

31 Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), p. 67. All of chapter 4 is devoted to this theme.

32 Nathan Woodard, "Tasting the Forbidden Fruit: Unlocking the Potential of Positive Politicization," *Intelligence and National Security* 28, no. 1 (February 2013), pp. 91-108.

33 Josh Kerbel and Anthony Olcott, "The Intelligence-Policy Nexus: Synthesizing with Clients, Not Analyzing for Customers," *Studies in Intelligence* 54, no. 4 (December 2010), p. 5-7.

34 See David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Intelligence University Press, 2011), pp. 64, 66.

35 In 2009, for example, the U.S. Director of National Intelligence declared that "The primary near-term security concern of the United States is the global economic crisis and its geopolitical implications." See Senate Select Committee on Intelligence, Intelligence Community Annual Threat Assessment, February 2009, p. 2, *http://intelligence.senate.gov/090212/blair.pdf*. Accessed 30 November 2012.

36 See *http://www.egmontgroup.org/*. Gregory F. Treverton foresaw the relevance of nongovernment institutions in the realm of financial intelligence in his "Intelligence and the Market State," *Studies in Intelligence* 10 (Winter/Spring 2001).

37 Cedric Chaffaut, "La unión europea, la geoeconomía y el patriotismo," Aainteligencia (edición impresa) 1, no. 3 (March 2008): 50-53.

38 William J. Bernstein, *A Splendid Exchange: How Trade Shaped the World* (New York: Atlantic Monthly Press, 2008).

39 Russell G. Swenson and Susana C. Lemozy, *Democratizacion de la Funcion de Inteligencia: El Nexo de la Cultura Nacional y la Inteligencia Estrategica* (Washington, DC: National Defense Intelligence College, 2009), p. Xxvi, *www.ni-u.edu/ni_press/pdf/Democratización_de_la_Función_de_Inteligencia.pdf*.

40 See Timothy Connors, "Putting the "L" into Intelligence-Led Policing: How Police Leaders Can Leverage Intelligence Capability," *International Journal of In-*

telligence and CounterIntelligence 22, no. 2 (Summer 2009), pp. 237-245. Also Christopher Dickey, *Securing the City: Inside America's Best Counterterror Force—the NYPD* (New York: Simon and Schuster, 2009).

41 As documented in Mark Riebling, *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994).

42 Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007), p. 172.

43 Michael D. Bayer, *The Blue Planet, op. cit*.

44 *Ibid.*, pp. 109-111.

45 See Kevin Wirth, *The U.S. Coast Guard Programs Enters the Intelligence Community* (Washington, DC: National Defense Intelligence College, 2007), *http://www.ni-u.edu/ni_press/pdf/The_Coast_Guard_Intelligence_Program%20.pdf*; Eric Ensign, *Intelligence in the Rum War at Sea, 1920-1933* (Joint Military Intelligence College, 2001), *http://ni-u.edu/ni_press/pdf/Intelligence_RUM_WAR.pdf*; and Martin Edwin Andersen, "A Roadmap for Beating Latin America's Transnational Criminal Organizations," *Joint Force Quarterly* 62 (July 2011), p. 86, *www.ndu.edu/press/latin-america-transnational-criminal.html*. Accessed 4 August 2012.

46 For example, see a review of local Mexican police practice in the Swenson-Orozco essay in this volume, in the section on "The Police Intelligence Model for Professional Accountability and Oversight," as well as the observations of James E. Steiner, in "Improving Homeland Security at the State Level: Needed—State-Level Integrated Intelligence Enterprises," *Studies in Intelligence* 53, no. 3 (October 2009), *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-53-no.-3/improving-homeland-security-at-the-state-level.html*. Accessed 10 August 2012.

47 Leslie A. Donovan, "Citizens as Intelligence Volunteers: The Impact of Value Structures," *International Journal of Intelligence and CounterIntelligence* 18 (Summer 2005), p. 241.

48 Andersen, *op. cit*.

49 Mario Villarreal Díaz and Juan José Rico Urbiola, "La penalización de las actividades de inteligencia hostil en los órdenes subnacionales de gobierno en México: el caso 'Nuevo León,'" in Jose Julio Fernandez Rodriguez *et al., Cuestiones de Inteligencia en la Sociedad Contemporánea* (Madrid: Ministerio de Defensa, Instituto

Español de Estudios Estratégicos, 2011), pp. 175-185, *http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/Cuestiones_inteligencia.pdf*. Accessed 10 August 2012.

50 For an example from Mexico, see Efrain Medina Valenzuela, "La inteligencia como herramienta facilitadora del trabajo policial," AAinteligencia (March 2007), *http://www.aainteligencia.cl/?p=220*. Accessed 12 August 2012.

51 Mark Ungar, *Policing Democracy: Overcoming Obstacles to Citizen Security in Latin America* (Washington, DC: Woodrow Wilson Center Press, 2011), p. 67.

52 Mark Ungar, "The Privatization of Citizen Security in Latin America: From Elite Guards to Neighborhood Vigilantes," *Social Justice* 34, nos. 3-4 (2007), p. 23.

53 Lucia Dammert, "La inseguridad urbana en Argentina: Diagnóstico y perspectivas," pp. 283-315, in Fernando Carrión, ed., *Seguridad ciudadana, ¿espejismo o realidad?* (Quito: FLACSO Ecuador, 2002), pp. 301-307.

54 See Christopher Dickey, *Securing the City, op. cit*.

55 Jeff Stein, "NYPD Intelligence Detectives Go Their Own Way," *Washington Post*, 10 November 2010, *http://voices.washingtonpost.com/spy-talk/2010/11/nypds_foreign_cops_play_outsid.html*. Accessed 11 August 2012.

56 Mark Munson, "Assessing the New York Police Department's Intelligence Efforts Targeting American Muslims," *Small Wars Journal* (March 2012), *http://smallwarsjournal.com/jrnl/art/assessing-the-new-york-police-department's-intelligence-efforts-targeting-america's-muslims*. Also see Small Wars Journal Editors, "NYPD Intelligence Division: The Homegrown Threat," *Small Wars Journal*, August 2007, *http://smallwarsjournal.com/blog/nypd-intelligence-division-the-homegrown-threat*. Both items accessed 11 August 2012.

57 U.S. Department of Justice, *The Attorney General's Guidelines for Domestic FBI Operations*, 29 September 2008, *http://www.justice.gov/ag/readingroom/guidelines.pdf*. Accessed 11 August 2012.

58 The 2001 "Patriot Act" (Public Law 107-56—Titles VII, VIII and IX) of the United States, enacted in the wake of the 9/11 attacks, as well as the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458—Title 1, section 1016) are examples. Similarly, Ecuadorian President Rafael Correa, in 2008, began a major overhaul of the Ecuadorian intelligence system apparently as a result of his assessment of the uncoordinated Ecuadorian intelligence approach to the

Colombian incursion against a FARC base in Ecuadorian territory in March of that year.

59 Russell G. Swenson, "Intelligence Education in the Americas," *International Journal of Intelligence and CounterIntelligence* 16, no. 1 (Spring 2003): 108-130.

60 See, for example, the opportunity mentioned on the web page of the Intelligence School of the Army of Chile, *http://www.escint.cl/* (under "Curso Extranjeros"), as presented on 11 September 2011.

61 Katitza Rodriguez, "The Politics of Surveillance: The Erosion of Privacy in Latin America," Electronic Frontier Foundation, 22 July 2011, *https://www.eff.org/deeplinks/2011/07/politics-surveillance-erosion-privacy-latin-america*. Accessed 11 August 2012.

62 Fernando Cocho Perez, "Aprender la historia, comprender el entorno, saber para cambiar," *Inteligencia y seguridad: Revista de análisis y prospectiva*, Madrid, no. 8 (June-November 2010). Inserted material is from the present author. Luis Iberico is a Peruvian congressman.

63 "Congressional Control of Intelligence Services…. Democratic States have various instruments and procedures through which the executive branch renders accountability to the legislative branch on behalf of the intelligence services…. The means used vary from country to country, but generally they are linked with revelations of irregular or failed actions in particular cases. No general rules exist concerning the nature or limitations of such control, given the need that exists for knowledge of and administrative oversight of intelligence activities by democratic representatives in each country, as well as the continuing need to preserve and protect the secret aspects of intelligence products and activities, in addition to protecting the means or methods and sources of information used in its production," from Miguel Ángel Esteban Navarro, coord., *Glosario de Inteligencia* (Secretaría General Técnica del Ministerio de Defensa de España, Imprenta Ministerio de Defensa de España, 2007), p. 66.

64 "Judicial Control of Intelligence Services…. Norms, procedures and organizations through which those who oversee the application of legal principles in general and the rights and liberties of citizens in particular act on behalf of intelligence services in carrying out their functions…." *Ibid*., p. 65.

65 "Economic Control of Intelligence Services…. Norms, procedures and organizations through which intelligence services render accountability for budget

expenditures and miscellaneous costs associated with the exercise of their official function.…" *Ibid*., p. 65.

66 Diego Navarro Bonilla, *¡Espías¡ Tres mil años de información y secreto* (Madrid: Plaza & Valdez, 2009), p. 122.

67 See Fernando Rospigliosi, *Montesinos y las Fuerzas Armadas: Cómo controló durante una década las instituciones militares*, first edition (Lima: IEP, December 2000), pp. 70-73. Also see Jorge Rodriguez Beruff, *Los militares y el poder—Un ensayo sobre la doctrina militar en el Perú: 1948–1968*, first edition (Lima: Mosca Azul editores, 1983) and Dirk Kruijt, *La Revolución por Decreto: El Perú durante el gobierno militar*, Democracy and Armed Forces series, no. 9 (Lima: Instituto de Defensa Legal, 2008).

68 In both the 27 January and 30 September 1960 documents, the signature of the president of the republic appears, along with the opinion of several state ministers and the express approval of the Council of Ministers.

69 A supreme decree is "a norm drafted and approved by the highest level of the Executive Branch, namely the President of the Republic…," from Marcial Rubio Correa, *El Sistema Jurídico: Introducción al Derecho*, sixth edition, corrected and updated (Lima: Fondo Editorial Pontificia Universidad Católica del Perú, 1993), p. 140.

70 Victor Garcia Toma, *La ley en el Perú: Técnica de elaboración, interpretación, aplicación e integración*, first edition (Lima: Editorial Jurídica GRIJLEY, February 1995), p. 49.

71 Acronyms, in their order of appearance in this paragraph, expand to *Secretaría de Inteligencia, Servicio Federal de Informaciones, Dirección Federal de Seguridad, Servicio de Inteligencia Colombiana, Departamento Administrativo de Seguridad, Dirección Nacional de los Servicios de Inteligencia y Prevención, Comité de Organización Política Electoral Independiente* (a political party).

72 Gustavo Gorriti, *Sendero: Historia de la guerra milenaria en el Perú* (Lima: Planeta, 2008).

73 This assertion by the present author is based on material presented in Dirk Kruijt and Maria del Pilar Tello, "De los reformistas militares a la dictadura civil: La política militar peruana desde los años sesenta hasta el presente," in Kees Koonings and Dirk Kruijt, eds., *Ejércitos Políticos: Las Fuerzas Armadas y la Construcción de la Nación en la Era de la Democracia*, American Problems series, no. 17, translated

by Gabriela Ramos, first edition (Lima: Instituto de Estudios Peruvianos—IEP, 2003), p. 97.

74 Anna Funder, STASILAND: *Historias del otro lado del Muro de Berlín* (Madrid: Tempus, 2009), p. 73.

75 Luis Piscoya, "Inteligencia en el Perú: conceptos organizativos y manejo de crisis," in various authors, *Apuntes para una nueva visión de la Seguridad Nacional* (Lima: Instituto de Estudios Políticos y Estratégicos–IDEPE, 2004).

76 See Andres Gomez de la Torre, "Del SIN al CNI y la DINI," in Andres Gomez de la Torre, comp., *SIN Arcana Imperii: Inteligencia en democracia*, first edition (Lima: Foro Libertad & Seguridad, 2007), pp. 93-94.

77 J. Patrice McSherry, *Los Estados depredadores: la Operación Cóndor y la guerra encubierta en América Latina* (Santiago de Chile: LOM ediciones, 2009).

78 "Article 21–National intelligence service personnel will certify their employment status with an identity card, which will facilitate access to all facilities, public and private. Managers of these facilities will allow access or face legal consequences, and will make information and any required assistance available to the agents for their mission accomplishment," in Legislative Decree No. 746, *Ley del Sistema de Inteligencia Nacional.*

79 Dirk Kruijt and Maria del Pilar Tello, *op. cit* skillfully recreate this stretch of Peruvian intelligence history.

80 See Fernando Rospigliosi, *Montesinos y las Fuerzas Armadas: Cómo controló durante una década las instituciones militares* (Lima: IEP, 2000); Carlos Iván Degregori, *La década de la antipolítica: Auge y huida de Alberto Fujimori y Vladimiro Montesinos* (Lima: IEP, 2001); Jane Marcus-Dalgado and Martin Tanaka, *Lecciones del final del fujimorismo*, Colección Mínima (Lima: IEP, 2001), p. 47.

81 Alberto Bolivar Ocampo, "Prefacio," in Russell G. Swenson and Susana C. Lemozy, coords., *Profesionalismo de Inteligencia en las Américas*, revised edition (Washington, DC: Joint Military Intelligence College, 2004), pp. 11-12. Added material by the present author.

82 As specified by the national constitution, an organic law regulates certain sensitive matters. This type of law occupies a position between the constitution itself and ordinary laws. Generally, organic laws require absolute or qualified majority approval. See *http://es.wikipedia.org/wiki/Ley_Org%C3%A1nica*.

83 Andres Gomez de la Torre, "Perú: Frustraciones en los intentos por reconstruir su sistema de inteligencia," in Russell G. Swenson and Susana C. Lemozy, coords., *Profesionalismo de Inteligencia en las Américas*, revised edition (Washington, DC: Joint Military Intelligence College, 2004), pp. 155-185.

84 The *Defensoría del Pueblo* is a governmental entity created by the Peruvian Constitution of 1993 to protect human rights in the country.

85 Defensoría del Pueblo, "*La Reforma y el control de los Servicios de Inteligencia," Revista de la Defensoria del Pueblo, Debate Defensorial*, no. 3 (May 2001), *http://www.defensaydemocracia.org/uploads/2/0/5/7/2057202/defensoria-pueblo_reforma-control-servicios-inteligencia.pdf*. Accessed 12 February 2012.

86 Law 27479, *Ley del Sistema de Inteligencia Nacional (SINA)*, 11 June 2001. "Article 36- Oversight: The role of the Select Committee for Intelligence of the Peruvian Congress is to oversee the operation and execution of the budgetary resources of the National Intelligence Council, in accordance with constitutional norms, Congressional regulations, and existing legal requirements." Temporary Provision: "The National Defense, Internal Order and current Intelligence Committees of Congress will carry out the functions of oversight until the creation of the Select Committee for Intelligence."

87 An extraordinary and perilous degree of similarity exists between Articles 4 and 8 of Law 27479 (2001), and Articles 2 and 4 of Law 25635 (1992). Andres Gomez de la Torre, "Evolución reciente y contextos de la legislación de inteligencia: El caso del Perú," in Laura Chamorro, ed., *Sistemas de inteligencia comparados: Aportes al caso peruano,* primera edición (Lima: IDEPE, 2010), pp. 37-116.

88 "The only justifiable secrecy for a State … is that which not only imposes silence, but which also maintains a judicious reticence with respect to topics in which silence is advisable, even if it has not been strictly imposed. Loyalty to the public interest and allegiance to public officials and their associates requires the careful exercise of judgment about what is said and not said, even though it is often the case that there is no formal requirement to safeguard the information…." from Sir Henry Taylor, "*The Statesman*" (1836), reproduced in John Gross, *Oxford Book of Essays* (New York: Oxford University Press, 1991), *http://www.nexos.com.mx/?P=leerarticulo&Article=111976*. Accessed 8 February 2012.ra

89 See the previous work of Jose Manuel Ugarte, *Legislación de inteligencia: Legitimidad y eficacia* (Guatemala: Washington Office on Latin America and Asociacion para el Estudio y Promoción de la Seguridad en Democracia, 2000). Ugarte, together with

Jaime Garreta and Marcelo Fabian Sain, were the chief promoters and architects of National Intelligence Law 25520 (2001) in Argentina.

90 See *Resolución Suprema No. 097-2004-PCM, Constituyen Comisión Especial encargada de implementar medidas aprobadas para la reestructuración del Consejo Nacional de Inteligencia*, published in the official newspaper *El Peruano*, 22 March 2004.

91 Peru, *Ley del Sistema de Inteligencia Nacional y de la Agencia de Inteligencia Estratégica, http://www.idepe.org/pdf/proyecto_inteligencia.pdf*. Accessed 12 March 2012.

92 For coverage of this topic, see Andres Gomez de la Torre, "Comisiones reformadoras de inteligencia: experiencias latinoamericanas recientes (2001-2009)," in Fredy Rivera Velez, *Inteligencia Estrategica y Prospectiva, op. cit.*, pp. 185-186.

93 *Ley del Sistema de Inteligencia Nacional–SINA y de la Dirección Nacional de Inteligencia–DINI*, Ley 28664, *http://www.congreso.gob.pe/ntley/Imagenes/Leyes/28664.pdf*. Accessed 10 March 2012.

94 "Special Operations. Intelligence and counterintelligence operations that often intrude on some citizens' rights, to protect against threats to national security, and requiring judicial pre-authorization to carry out." In *Ley del Sistema de Inteligencia Nacional—SINA y de la Dirección Nacional de Inteligencia–DINI, Ley no. 28664*, Primera Disposición Complementaria, Glosario.

95 Law 28664, *http://www.congreso.gob.pe/ntley/Imagenes/Leyes/28664.pdf*. Accessed 6 March 2012. The UIF-PERÚ participates as a member of *The Egmont Group of Financial Intelligence Units*. "The objective of the Egmont Group is to provide a forum for Financial Intelligence Units across the world to improve cooperation in the fight against money laundering and terrorism financing, and to promote national programs for doing so." See *http://www.egmontgroup.org/*. Accessed 6 March 2012.

96 Through Law 29038, the Financial Intelligence Unit of Peru (UIF-PERÚ) was placed under the Superintendent of Banking, Insurance and Private Administrators of Pension Funds (SBS).

97 For background on the "*MARTE-DINTEMAR*" case of selling intelligence information, see *http://www.desdeeltercerpiso.com/cat/carlos-barba/*. Accessed 9 March 2012. For the "*BTR*" case, see *http://www.larepublica.pe/06-10-2011/caso-btr-gustavo-gorriti-cuenta-la-historia-de-los-correos-truchos* Accessed 9 March 2012.

98 See Chapter 2 of Law 28664, especially Articles 14, 15, and 16, and Chapter 3 of title 2, especially Articles 20 and 21.

99 See Articles 3 and 5 of Law 28664.

100 This working group was created under the auspices of congressional regulations, which have the force of law and regulate the activities and functions of select committees.

101 This report resides in the archives of the Peruvian Congress.

102 According to the Strategic Intelligence Handbook of the SINA, information notes are to be prepared "in a precise, clear and concise format, answering the principal questions of What, Who, When, Where, How and Why or For What Purpose, and Intelligence Notes are the last step in information processing." See *Manual de Inteligencia Estratégica del SINA*, Tomo I, Escuela de Inteligencia Nacional–ESIN, 1994, pp. 56, 74.

103 Bill 2563-2007-CR, modifying Law 28664, Ley del Sistema de Inteligencia Nacional–SINA y de la Dirección Nacional de Inteligencia–DINA, *http://www2.congreso.gob.pe/Sicr/TraDocEstProc/CLProLey2006.nsf*. Accessed 6 March 2012.

104 On judicial control, see Brazil, Law 9883, art. 3, paragraph 1; Argentina, Law 25520, Title VI, art. 18–22; Chile: Law 19974, Title V, art. 23–32. On congressional control, see Brazil, Law 9883, art. 6; Argentina, Law 25520, Title VIII, art. 31–41; Chile, Law 19974, Title VI, art. 33–37.

105 On transparency of intelligence information, see items about the capture of "Artemio" Gustavo Gorriti, "*Crepúsculo en la madrugada," Caretas* magazine, *http://www.caretas.com.pe/Main.asp?T=3082&S=&id=12&idE=1000&idSTo=0&idA=57237&NL=1* and "*Cazando a 'Artemio*'," *Caretas*, *http://www.caretas.com.pe/Main.asp?T=3082&S=&id=12&idE=1000&idSTo=0&idA=57238*. Accessed 9 March 2012.

106 On this theme, see the work of Jose Manuel Ugarte, "El control de la actividad de Inteligencia: Realidad actual y tendencias hacia el futuro—Un análisis centrado en América Latina," paper presented at Santiago de Chile, Center for Hemispheric Defense Studies, REDES 2003; also see Andres Gomez de la Torre, "Servicios de Inteligencia y democracia en América del Sur. ¿Hacia una segunda generación de reformas normativas?," *Agenda Internacional*, Año XVI, no. 27 (Lima: Instituto de Estudios Internacionales, Pontifica Universidad Catolica, 2009), pp. 119-130.

107 *Decreto Ley no. 9*, 20 August 2009, *http://www.gacetaoficial.gob.pa/pdfTemp/26109/GacetaNo_26109_20080822.pdf*. Accessed 12 March 2012.

108 See Bill No. 26, 12 August 2009, *http://www.asamblea.gob.pa/apps/seg_legis/PDF_SEG/PDF_SEG_2000/PDF_SEG_2009/2009_P_026.pdf*. Accessed 12 March 2012.

109 On 5 March 2010, the Colombian Jurist Commission (CCJ) and the *Reiniciar* Corporation asserted the unconstitutionality of this law because of a series of missteps in the formation of the law, as well as in the wording of various articles in the law. A summary of this challenge to the law is at *http://www.coljuristas.org/Portals/0/S%C3%ADntesiseligencia.pdf*. Accessed 29 November 2010.

110 For perspective on the Colombian espionage case and the unconstitutionality of the Law of Intelligence and Counterintelligence as declared by the Constitutional Court, see Alejo Vargas Velasquez, "La Inteligencia está de moda," *El Colombiano.com* (2010), *http://www.elcolombiano.com//BancoConocimiento/L/la_inteligencia_esta_de_moda/la_inteligencia_esta_de_moda.asp*. Accessed 2 December 2010.

111 Andres Gomez de la Torre and Raul Santiago Calle Pena, *Inteligencia en los Andes: Avances y retrocesos* (El Alto, Bolivia: Centro Andino de Estudios Estratégicos, July 2011), p. 6, *http://www.resdal.org/producciones-miembros/inteligencia-en-los-andes2.pdf*. Accessed 12 March 2012.

112 See "Agencia que reemplaza al DAS no será policial," *http://www.elpais.com.co/elpais/colombia/noticias/agencia-reemplaza-das-sera-policial*. Accessed 10 February 2012.

113 "The National Intelligence Directorate will have an Inspector General who will oversee compliance with the law," *http://wsp.presidencia.gov.co/Prensa/2011/Noviembre/Paginas/20111104_15.aspx*. Accessed 9 March 2012.

114 "Angostura marcó un antes y un después en las FFAA," *Hoy.com*, 15 January 2009, *http://www.hoy.com.ec/noticias-ecuador/angostura-marco-un-antes-y-un-despues-en-las-ffaa-328808.html*. Accessed 9 March 2012.

115 These principles are addressed in the cited bill: "Article 4—In the collection and handling of information, intelligence officials must ensure that their actions conform with the following principles: *Legitimacy* (full conformation with the law, with actions in line with an organization's intrinsic responsibilities). *Efficiency* (appropriate relationship between available means and the quality and value of the intelligence product). *Financial probity* (appropriate sourcing and use of funds

allocated to the intelligence services, to include those for 'black programs'). The strict observance of *legality* in those procedures that inevitably require invading the privacy of individuals. The strict observance of the principles of '*need to know*' and '*need to share*' in the correct and complete execution of the functions (principles) defined above. Finally, ensuring that information not be used for the benefit of a particular person, private organization, or any political party."

116 Decree 6067 (abrogated), with rank, value and force of law, of the National Intelligence and Counterintelligence System, *Gaceta Oficial de la República Bolivariana de Venezuela* no. 38940, 28 May 2008.

117 On SEBIN, see *http://www.intelpage.info/servicio-bolivariano-de-inteligencia-nacional-sebin.html*. Accessed 9 March 2012.

118 For more information, see Andres Gomez de la Torre Rotta, "Comisiones reformadoras," *op. cit.*, pp. 190-191.

119 This evolutionary or developmental path has passed through the following stages: "a) scandal; b) development and establishment of an evaluative/investigative commission; c) final report of a commission that included conclusions and recommendations, among them the need for a normative framework to reinforce the new approach; d) legislative bill, usually prepared by the executive branch (Ecuador, Costa Rica), and/or with inputs from other bills presented in congress (Peru, Colombia); and e) new normative framework with emphasis on intelligence laws that incorporate checks and balances with respect to the legislative branch relationship with intelligence services (external control) and judicial branch (parallel control)," cited in Andres Gomez de la Torre Rotta, "Servicios de Inteligencia," *op. cit.*, p. 127. Also see Andres Gomez de la Torre Rotta, "Comisiones reformadoras," *op. cit.*, pp. 179-180.

120 This theme is developed in Andres Gomez de la Torre Rotta, "Comisiones reformadoras," *op. cit.*, pp. 177-196.

121 "Social control is probably the most important of all, because it involves the independent scrutiny that the press, political parties, public opinion, academia, and think tanks can bring to bear," cited in Carlos Maldonado, "Desafíos de los servicios de inteligencia en la región andina," in Andres Gomez de la Torre Rotta, comp., *SIN Arcana Imperii. Inteligencia en democracia* (Lima: Foro Libertad & Seguridad, 2007), p. 273.

122 For example, see Jose Julio Fernandez Rodriguez and Daniel Sanso-Rubert Pascual, "El recurso constitucional a las fuerzas armadas para el mantenimiento de

la seguridad interior: el caso de Iberoamérica," *Boletín Mexicano de Derecho Comparado* of the Instituto de Investigaciones Jurídicas-UNAM, XLIII, no. 128 (May-August 2010), pp. 737-760. Also see Kate Martin, "Domestic Intelligence and Civil Liberties," *SAIS Review*, XXIV, no. 1 (Winter-Spring 2004), pp. 7-21. In the Peruvian case, Bill 1374/2006-PE, and Report 17 on this bill, permitted the enactment of Law 29166, titled "Law establishing rules for the use of force by members of the armed forces in the national territory." This law established the Peruvian legislative tendency to delegate to the armed forces those tasks related to internal order or support in the establishment of that order. See *http://www.congreso.gob.pe/ntley/Imagenes/Leyes/29166.pdf*. Accessed 13 March 2012.

123 The executive branch was granted a period of 90 days to develop legislation strengthening and modernizing the National Security and Defense System (Legislative Decree 1141). See *http://www.mef.gob.pe/contenidos/servicios_web/conectamef/pdf/normas_legales_2012/NL20120912.PDF*.

124 The proposals were: 721/2012-CR, 722/2012-CR, 724/2012-CR, 728/2012-CR, and 730/2012-CR.

125 For the full text of the decree, see *http://dataonline.gacetajuridica.com.pe/gaceta/admin/elperuano/2012-11-12/11-12-2012.PDF*.

126 Theoretically, the Peruvian Congress could find the legislative decree unconstitutional, but barring such a development, the enactment of the decree remains in executive branch hands.

127 Jose Manuel Ugarte, "Controle Público da Atividade de Inteligência: a Procura de Legitimidade e Eficácia," in Brazilian National Congress, *Anais do Seminário Atividades de Inteligência no Brasil: Contribuições para a Soberania e a Democracia*, 6-7 November 2002 (Brasília: Agência brasileira de inteligência/Abin, 2003), pp. 89-145.

128 Thomas Bruneau, "Intelligence and Democratization: The Challenge of Control in New Democracies," *Occasional Paper no. 5* (Monterey, CA: *The Center for Civil-Military Relations–Naval Postgraduate School*, March 2000).

129 Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994).

130 The word "inteligência" was incorporated into Brazilian doctrine at the beginning of the 1990s, following redemocratization, as a substitute for the term "informações," which is more commonly used in the Portuguese language. The main

reason for the adoption of the new term was political, part of an attempt to ban terminology associated with the military regime. Another example is the disuse of the term "national security." To be clear, "informações" is still used in Brazil, and is understood to be the equivalent of "intelligence," but is not the same thing as "informação," which refers to information gathered in relation to a particular issue. For more on these distinctions, see the author's *Atividade de Inteligência e Legislação Correlata*, second edition (Niterói: Impetus, 2011).

131 Despite the fact that some authors who write about intelligence in Brazil write of "covert actions" and "clandestine actions," these terms are completely alien to Brazilian intelligence doctrine; they are not used by intelligence professionals. In Brazil, one speaks only of "intelligence operations."

132 In antiquity, in his classic work on strategy, *A Arte da Guerra* (Rio de Janeiro: Bibliex, 2003), the Chinese general Sun Tzu (fourth century BCE) addresses the importance that generals and governors attach to employing spies.

133 For more extensive coverage of the issues surrounding the control of intelligence activity, to include the topics addressed in the present paper, see the author's *Políticos e Espiões–o controle da atividade de inteligência* (Niterói, Brazil: Impetus, 2010).

134 Hely Lopes Meirelles, *Direito Administrativo Brasileiro*, twenty-first edition (São Paulo: Malheiros, 1996), p. 574.

135 Meirelles, *ibid*., p. 574.

136 Celso Antônio Bandeira de Mello, *Curso de Direito Administrativo*, thirteenth edition (São Paulo: Malheiros, 2001), p. 212.

137 Meirelles, *op. cit*., p. 576.

138 Jans Born, "Towards Effective Democratic Oversight of Intelligence Services: Lessons Learned from Comparing National Practices," *Connections–A Quarterly Journal*, 3 (December 2004), p. 4.

139 Greg Hannah, Kevin O'Brien, and Andrew Rathmell, *Technical Report: Intelligence and Security Legislation for Security Sector Reform*, prepared for the United Kingdom's Security Sector Advisory Team, (Cambridge, RAND Europe, June 2005), p. 12.

140 In the Anglo-Saxon world, the concept of accountability combines with ethics within intelligence services and therefore applies to the decisions of individual practitioners.

141 Curiously, another English term that has no direct counterpart in Portuguese is "enforcement."

142 For more on the principles that guide Brazilian public administration, see Bandeira de Mello, *op. cit.*, Chapter II; Meirelles, op. cit., pp. 82-87; also Fernanda Marinela, *Direito Administrativo*, fourth edition (Niterói: Impetus, 2010), pp. 26-63.

143 Geneva Centre for the Democratic Control of Armed Forces (DCAF), DCAF *Intelligence Working Group, Intelligence Practice and Democratic Oversight–A Practitioner's View, DCAF Occasional Paper no. 3* (Geneva, July 2003), p. 1.

144 From the individual in charge of a particular operation to the director general, through the entire chain of supervisors of the office or department, everyone has the obligation to exert managerial control over his or her subordinates.

145 "… the secrecy surrounding the intelligence function makes exercising control problematic." From Glenn P. Hastedt, ed., *Controlling Intelligence* (London: Frank Cass, 1991), p. 13.

146 DCAF Intelligence Working Group, *op. cit.*, p. 2.

147 "Even in old and stable democracies leaders often prefer 'plausible deniability' rather than access to the information required to control a potentially controversial or dangerous organization or operation. Logically this would be even more the case in newer democracies. First, the politicians may be afraid of antagonizing the intelligence apparatus through efforts to control it because the intelligence organization might have something embarrassing on them. Second, they may be afraid because the intelligence organization in the past engaged in arbitrary and violent actions and the politicians are not sure that a corner has been turned. Third, there are probably no votes to be won in attempting to control an organization that most people want to ignore." From Bruneau, *op. cit.*, pp. 23-24.

148 Thomas Bruneau and Steven Boraz, eds., *Reforming Intelligence–Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), p. 13.

149 Hastedt, *op. cit.*, pp. 14-15.

150 Ugarte, "Controle Público da Atividade de Inteligência,"*op. cit.*, p. 102.

151 Marina Caparini, "Challenges of Control and Oversight of Intelligence Services in a Liberal Democracy," Geneva Centre for the Democratic Control of Armed Forces, Conference paper presented at the Workshop on Democratic and Parliamentary Oversight of Intelligence Services, Geneva, 2002.

152 Bruneau and Boraz, *op. cit.*, pp. 12-13.

153 Marina Caparini, *op. cit.*

154 Mary Sturtevant, "Congressional Oversight of Intelligence: One Perspective," *American Intelligence Journal* (Summer 1992), *http://www.fas.org/irp/eprint/sturtevant.html*. Sturtevant was a member of the U.S. Senate Select Committee on Intelligence.

155 Amy B. Zegart, "The Domestic Politics of Irrational Intelligence Oversight," *Political Science Quarterly*, 126, 1 (Spring 2011).

156 Zegart, *ibid.*, p. 9.

157 Reg Whitaker, "Designing a Balance between Freedom and Security," in Joseph Fletcher, ed., *Ideas in Action: Essays on Politics and Law in Honour of Peter Russell* (Toronto: University of Toronto Press, 1999), pp. 144-145.

158 Caparini, *op. cit*.

159 Zegart, *op. cit*.

160 Peter Gill, "Security and Intelligence Services in the United Kingdom," in Jean-Paul Brodeur and Dennis Tollberg, eds., *Democracy, Law and Security–Internal Security Services in Contemporary Europe* (Aldershot, UK: Ashgate Publishing Limited, 2003), p. 4.

161 Jose Manuel Ugarte, "Control público de la actividad de inteligencia: Europa y América Latina, una visión comparativa," paper presented at international seminar on Post-Globalización: Redefinición de la Seguridad y la Defensa Regional en el Cono Sur, organized by Centro de Estudios Internacionales para el Desarrollo, in Buenos Aires, 2002.

162 Peter Gill, Policing *Politics: Security Intelligence and the Liberal Democratic State* (London: Frank Cass, 1994), p. 251.

163 In Romano-Germanic judicial systems, an effective legal framework anchors the actions of public officials, because, in terms of public administration, "whatever is not spelled out in law, does not exist." This significantly affects the discretion of officials in public administration. Further, specific behaviors of public officials need to be anticipated by legal disposition. Brazil's judicial-legal system is not only bound to the Romano-Germanic tradition, but is also strongly influenced by nineteenth-century positivism. This means that private citizens can do whatever is not expressly prohibited by law. At the same time, in the public sphere, one can only do what is expressly authorized by law. Brazilian history exhibits "exceptional" regimes that legitimize their actions through the establishment of new legal frameworks. Thus, in Romano-Germanic systems, new laws and authorizations can come to support abusive actions by public officials.

164 Peter Gill, "A Inteligência, Controle Público e Democracia," translation by Maria Isabel Taveira, in Brazilian National Congress, *Anais do Seminário Atividades de Inteligência no Brasil: Contribuições para a Soberania e a Democracia*, 6-7 November 2002 (Brasília: Abin, 2003), p. 70.

165 Gill, *ibid*., p. 79.

166 Among the sources for the synthesis presented here are the Council of Europe's Geneva Centre for the Democratic Control of Armed Forces' (DCAF) recently published works featuring case studies of the control of intelligence activities from around the world, and the practical experience of the author. More detailed information on approaches to and practices in intelligence control are available in the author's book *Políticos e Espiões–o controle da atividade de inteligência, op. cit*.

167 Thomas Bruneau and Kenneth Dombroski, "Reforming Intelligence: The Challenge of Control in New Democracies," *http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/bruneau.pdf*, pp. 16-17.

168 For an example, one may consult the web page for BfV, Germany's domestic intelligence service, where the service identifies the threats it engages: *http://www.verfassungsschutz.de*. Accessed 11 October 2011.

169 The difficulty of doing so appears, for example, in the U.S. intelligence system, with the division of responsibilities between the Central Intelligence Agency and the Federal Bureau of Investigation, and limitations on the activity of the National

Security Agency. Despite improvements in the implementation of certain actions in the realm of counterintelligence, conflicts in jurisdiction, as noted by Mark Riebling, have not yet been resolved. See his *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994).

170 To understand the full intent of the law, and of the decree that it implements, see *https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm* (in Portuguese).

171 On this point, see Senator and ex-President of the Republic Fernando Collor de Mello's comments on House Bill 41 (of 2010), which began the process leading to the Law on Access to Information (LAI), *http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=96674* and *http://joanisval.com/2012/05/26/ainda-sobre-a-lei-de-acesso-a-informacao/*. Also please see the author's technical comments on the law on his web page (*www.joanisval.com*).

172 For the Mexican *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, see *www.diputados.gob.mx/LeyesBiblio/doc/244.doc*.

173 On this issue, see *Mexico's Access to Information Index*, 29 April 2010, *http://www.article19.org/data/files/pdfs/press/mexico-access-to-information-index.pdf*, accessed 20 May 2012, and Ernesto Isunza-Vera, "O Sistema Mexicano de Transparência e Acesso à Informação Pública Governamental" (text prepared for the regional seminar "Sociedade civil e as novas institucionalidades democráticas na América Latina: dilemas e perspectivas," Brasília, 9-12 November 2008), *http://www.inesc.org.br/equipe/ivonem/MEXICO%20Acesso%20a%20informacao.pdf*. Accessed 24 May 2012.

174 According to Article 49 of the Brazilian Constitution, the National Congress has exclusive responsibility to "decide on treaties, accords or other international acts that involve duties or commitments that affect national heritage." Thus, any treaty signed by Brazil must be submitted for review to the House of Representatives and the Federal Senate prior to being ratified.

175 The decision of the CRE that established the precedent grew from the report of Senator Aloysio Nunes Ferreira on Bill 238, of 2011 (originally Bill 46, of 2011), which approved the text of the accord between Brazil and Spain concerning the security of classified information, signed in Madrid 17 September 2007. The text of the report is at *http://www6.senado.gov.br/mate-pdf/103774.pdf*. Accessed 1 May 2012.

176 The text of Law 9883 is found at *http://www.planalto.gov.br/ccivil_03/LEIS/L9883.htm* (in Portuguese).

177 The "gang of eight" is made up of the chairman and vice-chairman of the intelligence committees of the House and Senate, and by the majority and minority leaders of both houses.

178 National Security Act of 1947, as amended, Sec. 503 [50 U.S.C. 413b] (b) and (c).

179 On this topic, see "*Sensitive Covert Action Notifications: Oversight Options for Congress*," Congressional Research Service Report for Congress, R40691, 6 April 2011, *http://assets.opencrs.com/rpts/R40691_20110406.pdf* (accessed 1 January 2012), and "Gang of Four Congressional Intelligence Notifications," Congressional Research Service Report for Congress, R40698, 18 March 2011, *http://assets.opencrs.com/rpts/R40698_20110318.pdf* (accessed 1 January 2012), both by Alfred Cumming.

180 See L. Elaine Halchin and Frederick M. Kaiser, "*Congressional Oversight of Intelligence: Current Structures and Alternatives*," Congressional Research Service Report for Congress, RL32525, 14 March 2012, *http://assets.opencrs.com/rpts/RL32525_20120314.pdf*. Accessed 1 June 2012.

181 "Ministers are only rarely brought before full sessions of Congress.... Between 1988 and 2004, there were 201 appearances in the House and 126 in the Senate—a total of 344 in 16 years, or fewer than one appearance per Member of the House, and fewer than 1.5 in the Senate, despite the perception that the House is the most activist in this regard.... Appearances by Ministers and other authorities before Committees, where this is a common practice, are not included." Leany Barreiro Lemos, *Controle Legislativo em Democracias Presidencialistas: Brasil e EUA em perspectiva comparada*, doctoral dissertation (Brasília: Universidade de Brasília, 2005), p. 89.

182 "[Requests for Information] are made in written form and presented in a plenary session of both Chambers, where they are read and submitted to a vote, with approval by a simple majority. Requests for Information cannot contain a request for luck, advice, suggestions, counsel or questions about the purposes of the authority to whom it is directed; in all cases they must focus on the demand for documents. Refusal to comply with the request, or ignoring it for more than 30 days, as well as the provision of false information, is a crime.... Requests for Information, quantitatively speaking, are preferred [over forced appearances by a minister]: from

the promulgation of the Constitution in 1988 until 31 December 2004, 15,341 Requests for Information came from the House of Representatives, and 3,097 from the Federal Senate, for a total of 18,438." Lemos, *op. cit.*, p. 87.

183 "Addressed in Article 58 of the Federal Constitution of 1988, public hearings are held as much to bring public attention to certain issues as to exercise control of intelligence activity, and are used exclusively to engage civil society entities such as unions or associations, and to acquire the testimony of certain authorities or citizens." Lemos, *op. cit.*, pp. 91-92.

184 "An incentive for the use of Requests for Information is their low cost.… They do not alter the status quo and, thus, Congress does not run the risk of moving public policies in unanticipated directions.… That is not to say that this approach is not a real mechanism of control. It can be a strategic instrument when it tackles sensitive issues, negotiates legislative actions, or allocates resources." Lemos, *op. cit.*, pp. 87-88.

185 To avoid unnecessary discomfort among executive branch officials, an "invitation" rather than a "demand" is extended for them to attend public or private sessions with Congress. Executive officials, at least in the intelligence area, tend to appear before congress without hesitation. On this issue, see Lemos, *op. cit.*, and Maria Helena de Castro Santos, "Controles parlamentares e os militares no Brasil: audiências públicas e requerimentos de informações, 1995–2004," in Mariana Llanos and Ana Maria Mustapic (orgs.), *Controle Parlamentar na Alemanha, na Argentina e no Brasil* (Rio de Janeiro: Fundação Konrad Adenauer, 2005), pp. 113-139.

186 This has already occurred, for example, in Canada, when a committee of parliamentarians (and not a *Parliamentary committee or committee of Parliament*) was created to oversee issues related to the security and intelligence community. This committee turned out to have limited effect, and in fact acted in consonance with the interests and point of view of the Prime Minister. On this issue, see Stuart Farson, "Parliament and Its Servants: Their Role in Scrutinizing Canadian Intelligence," in David Stafford and Rhodri Jeffreys-Jones, eds., *American-British-Canadian Intelligence Relations 1939–2000* (London: Frank Cass, 2000), pp. 225-258.

187 On this topic, see Zegart, "The Domestic Politics of Irrational Intelligence Oversight," *op. cit.*

188 "6. (1) The Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith. (2) In providing the direction referred to in subsection (1), the Minister may issue to the Director

written directions with respect to the Service and a copy of any such direction shall, forthwith after it is issued, be given to the Review Committee." CSIS Act, section 6, (1), (2).

189 "The CSIS Act established, in law, a comprehensive regime for the security intelligence function in Canada: a civilian agency with no executive terms of reference; with clearly [and where appropriate, precisely] defined mandate and powers; subject to a rigorous, inter-related system of political and judicial controls; and, importantly, subject to independent, arm's-length review. The centrepiece of that system for accountability, control and review was and is the unique combination of the Security Intelligence Review Committee (SIRC) and the Inspector General (IG)—the former reporting through the Minister to Parliament; the latter, in a more specialized but complementary way, acting as the "Minister's 'eyes and ears' on the Service." Canadian Security Intelligence Service, *Backgrounder no. 17: Control, Accountability and Review,* May 2005, *http://www.csis.gc.ca/en/newsroom/backgrounders/backgrounder17.asp*. Accessed 25 February 2012.

190 "The Security Intelligence Review Committee is the only body with the legal mandate and expertise to carry out ongoing, independent review of the activities of CSIS. SIRC was established under the CSIS Act (1984) to provide assurance to the Parliament of Canada and to Canadians that CSIS is acting in accordance with the law, policy and ministerial direction in the performance of its duties and functions. In doing so, SIRC seeks to ensure that CSIS respects the fundamental rights and freedoms of Canadians." Security Intelligence Review Committee (SIRC), *SIRC Annual Report 2006–2007—An Operational Review of the Canadian Security Intelligence Service* (Ottawa: Public Works and Government Services Canada, 2007), p. 3.

191 "SIRC recognizes that the conduct of security intelligence agencies can prompt impassioned debate about whether the ends can ever justify the means. We also have first-hand knowledge that there are individuals who will seek to exploit Canada's rights and freedoms in order to harm our country, our citizens and our neighbours and friends around the world.… SIRC recognizes that police and security intelligence agencies in the post-9/11 world must deal with daunting challenges, including globalized and technologically sophisticated terrorist groups. We also know that the relative safety that Canadians enjoy is thanks in large part to the efforts of these same agencies on our behalf. But the obligation to ensure public safety ought not to reduce in any way respect for the rule of law." SIRC Annual Report 2006–2007, pp. v-vi.

192 "40. For the purpose of ensuring that the activities of the Service are carried out in accordance with this Act, and that the activities do not involve any unreasonable

or unnecessary exercise by the Service of any of its powers, the Review Committee may (a) direct the Service or Inspector General to conduct a review of specific activities of the Service and provide the Committee with a report of the review; or (b) where it considers that a review by the Service or the Inspector General would be inappropriate, conduct such a review itself." CSIS Act, Section 40.

193 CSIS Act, Sections 41 to 46.

194 Article15 of the National Defense Act of 1988 distinguished concepts of national defense and internal security, and prohibited the armed forces from engaging in internal security issues through intelligence activity related to domestic policy matters.

195 "Predator Drones and Unmanned Aerial Vehicles," New York Times, 30 July 2012 (updated), *http://topics.nytimes.com/top/reference/timestopics/subjects/u/unmanned_aerial_vehicles/index.html*. Accessed 15 August 2012. Also see Spencer Ackerman, "How the Pentagon's Top Killers Became (Unaccountable) Spies," *Wired* Magazine, 13 February 2012, *www.wired.com/dangerroom/2012/02/jsoc-ambinder/*. Accessed 15 August 2012.

196 Per U.S. Congress, Fiscal Year 2010 Intelligence Authorization Act, Public Law 111–259, 7 October 2010, Section 326, Subtitle D, *http://intelligence.senate.gov/pdfs111th/111259.pdf*. Accessed 15 August 2012.

197 The Foreign Intelligence Surveillance Act applies only to intelligence operations by agencies of the U.S. Intelligence Community inside of the United States. For an outline of the 1978 Act and its amendments, see the Center for National Security Studies site at *http://www.cnss.org/fisa.htm*. Accessed 15 August 2012.

198 Gregory Weeks, "A Preference for Deference: Reforming the Military's Intelligence Role in Argentina, Chile and Peru," *Third World Quarterly* 29, no. 1 (2008), p. 57.

199 "The term 'ethics' derives from the Greek word meaning 'custom,' and therefore ethics has often been defined as customary doctrine, especially by empiricists. For Aristotle, ethical virtues are developed through practice and are put in place to achieve a particular purpose, so that 'dianetics' may be thought of as rational 'social psychology.' In the subsequent evolution of the concept, ethics has come to be equated with morality, and to refer to the study of moral philosophy." Moreover, "just as 'ethics' derives from ήθος, 'moral' derives from *mos*, or 'custom,' and therefore the terms are often used interchangeably. In some languages, including Spanish, morality refers to the nonmaterial universe, so that unlike the physical

sciences, moral 'science' addresses anything not purely physical (such as history, politics, skills or abilities, etc.); that is, anything that is a product of the subjective spirit, as well as the subjective spirit itself. And, finally, morality is distinguished from immorality or amorality in the sense that whatever is found to be ethical is in conflict with what is not ethical or with anything that remains indifferent. Morality has value, whereas immorality or amorality are, respectively, without value or indifferent to value." From Jose Ferrater Mora, *Diccionario de la Filosofía*, fifth edition (Buenos Aires: Editorial Sudamericana, 1964), vol. I, pp. 594-595, and vol. II, pp. 232-233.

200 The list of authors is long. Many were or are members of the U.S. Intelligence Community. Others teach or conduct research in universities in North America or Western Europe, or are high-level officials of Western democracies. Some of them are cited in this work: Stefan Brem, Jan Goldman, Melvin Goodman, Albert Pierce, Erich Schimdt-Eenboom, and Brian Snow.

201 To date the IIEA has not, either in its conferences or its journal, included papers about Latin America. The present essay takes note of several publications from the IIEA's professional journal.

202 Allison M. Shelton, "Framing the Oxymoron: A New Paradigm for Intelligence Ethics," *Intelligence and National Security* 26, no. 1 (2011), p. 25.

203 Jan Goldman, "Ethics Phobia and the U.S. Intelligence Community: Just Say 'No', A Symposium on Intelligence Ethics," *Intelligence and National Security* 24, no. 3 (2009), p. 374. This author, then a professor of the National Defense Intelligence College in Washington, DC, labels as "ethics phobia" the fear of contemplating the topic of ethical behavior.

204 Shelton, *op. cit.*, pp. 28-30.

205 Shelton, *op. cit.*, p. 26.

206 Tony Pfaff and Jeffrey R. Tiel, "The Ethics of Espionage," *Journal of Military Ethics* 3, no. 1 (2004), pp. 11-14.

207 Pfaff and Tiel, *ibid.*, pp. 14-15.

208 Melvin A. Goodman, author of the book *Failure of Intelligence: The Decline and Fall of the CIA* (New York: Rowman & Littlefield Publishers, 2008).

209 Melvin A. Goodman, "Revamping the CIA," *Issues in Science and Technology Online* (Winter 2001), *http://www.issues.org/18.2/goodman.html*. Accessed 22 August 2012.

210 U.S. Senate, *Alleged Assassination Plots Involving Foreign Leaders: An Interim Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities* (Washington, DC: U.S. Government Printing Office, 20 November 1975), pp. 257-258, *http://www.aarclibrary.org/publib/church/reports/ir/pdf/ChurchIR_4_Findings.pdf*. Accessed 23 August 2012.

211 Elizabeth B. Bazan, *Assassination Ban and E.O. 12333: A Brief Summary*, Congressional Research Service Report RS21037 (Washington, DC: CRS, 4 January 2002), pp. 1-3.

212 Melvin A. Goodman, "CIA Failures of Tradecraft and Intelligence Prior to the Second Iraq War," in *Intelligence Ethics: The Definitive Work of 2007*, Michael Andregg, ed. (St. Paul, Minnesota: Center for the Study of Intelligence and Wisdom, 2007, p. 32, *http://www.gzmn.org/pdfonline/IntelligenceEthics2007-MA.pdf*. Accessed 23 August 2012.

213 Erich Schmidt-Eenboom, "Geheimdienste in Demokratien," *Welttrends: Zeitschrift für internationale Politik und vergleichende Studien* 14, no. 51 (2006), p. 17.

214 Schmidt-Eenboom, *ibid*., pp. 14-23.

215 Schlächter von Lyon, "Nazi-Verbrecher Barbie war BND-Agent," *Der Spiegel*, 15 January 2011, and Michael Kimmelman, "50 Years After Trial, Eichmann Secrets Live On," *New York Times*, 9 May 2011.

216 Stefan Brem, "Special Ethics for Special Services," in *Intelligence Ethics: The Definitive Work of 2007*, Michael Andregg, ed. (St. Paul, Minnesota: Center for the Study of Intelligence and Wisdom: 2007), pp. 11-13. All ten guidelines may be found at *http://www.echr.coe.int/NR/rdonlyres/176C046F-C0E6-423C-A039-F66D90CC6031/0/LignesDirectrices_EN.pdf*. Accessed 23 August 2012.

217 Schmidt-Eenboom, *op. cit*., p. 24.

218 Brian Snow, "Intelligence Community 'Mission Ethics': A Symposium on Intelligence Ethics," *Intelligence and National Security* 24, no. 3 (2009), p. 385.

219 "El CNI prepara un 'código ético' del agente secreto," *ABC*, Madrid, 25 June 2010.

220 "El código ético de los espías estará listo en primavera," *El Confidencial Digital*, Madrid, 7 March 2011.

221 "El código ético del CNI," *El Confidencial Digital*, Madrid, 12 January 2012.

222 Albert C. Pierce, "The Value of an Ethos for *Intelligence Professionals," in Intelligence Ethics: The Definitive Work of 2007, op. cit*., pp. 9-10.

223 Florina Cristiana Matei and Thomas Bruneau, "Explaining Failures and Successes in the Democratization of Intelligence," Panel on Politics of Intelligence Governance, The European Consortium for Political Research's General Conference, Potsdam, Germany: 10-12 September 2009, pp. 2-3.

224 Rafael Jose de Espona, "Los servicios de inteligencia en los países post-soviéticos," *Inteligencia y Seguridad* no. 8 (2010), p. 77.

225 Julia Pulido Gragera, *Los servicios de inteligencia rusos: Influencia de la nueva Rusia en el actual sistema de seguridad* (Madrid: Centro Superior de Estudios de la Defensa Nacional, 2010), pp.138-143.

226 Matei and Bruneau, *op. cit*., pp. 15 and following.

227 Carlos Maldonado Prieto, "Desafíos de los servicios de inteligencia en la región andina," in *SIN Arcana imperii: Inteligencia en democracia, op. cit*., p. 267.

228 Carlos Maldonado Prieto, "Dilemas antiguos y modernos en la inteligencia estratégica en Sudamérica," *Security and Defense Studies Review* 9 (2009), p. 54.

229 "Creación de nueva agencia nacional de inteligencia recibe apoyo del bobierno británico," *Radio Santa Fe*, Bogota, 9 November 2011. President Juan Manuel Santos of Colombia and his national security advisor, Sergio Jaramillo, met in London late in November 2011 with John Sawyer, director of MI6. See *http://unidad-intel-latinoamerica.webnode.com.ar/news/presidente-santos-crea-nueva-agencia-de-inteligencia-colombiana-con-apoyo-del-reino-unido-/*. Accessed 23 August 2012.

230 "Colombia crea una nueva agencia de inteligencia tras haber liquidado anterior," *EFE* (Spanish news service), 4 November 2011.

231 Article 4 also notes that in no case will intelligence or counterintelligence information be collected, processed, or disseminated for reasons of gender, race,

national or family origin, language, religion, political or philosophical opinion, membership in a social, labor, or human rights organization, to promote the interests of any political party or movement, or to affect the rights and guarantees of opposing political parties. See Ley de Inteligencia y Contrainteligencia de Colombia at *http://colarebo.files.wordpress.com/2011/05/ley-de-inteligenia-y-contrainteligencia-pdf.pdf*. Accessed 23 August 2012.

232 "Due obedience" was traditionally understood in Latin America as a stipulation exempting from criminal responsibility those crimes committed in carrying out an order given by a superior in the military environment, and which the subordinate could not refuse to carry out. However, after the military dictatorships of the 1970s and 1980s, the legal environment changed radically by adopting the approach of international humanitarian law, which does not recognize due obedience as an acceptable reason for exempting an individual from criminal responsibility.

233 Ley de Inteligencia y Contrainteligencia de Colombia, *http://colarebo.files.wordpress.com/2011/05/ley-de-inteligenia-y-contrainteligencia-pdf.pdf*. Accessed 23 August 2012.

234 Fredy Rivera, "La Inteligencia ecuatoriana: Tradiciones, cambios y perspectivas," in his *Inteligencia Estratégica y Prospectiva, op. cit*., pp. 62-63.

235 Rivera, *ibid*., pp. 59-60.

236 Carlos Maldonado Prieto, "La sublevación policial en Ecuador," *Revista Atenea Digital*, 2 October 2010., *http://www.ateneadigital.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_3055_ESP.asp*, and Carlos Maldonado Prieto, "Desafíos para la Inteligencia Estratégica Latinoamericana," *Revista Atenea Digital*, 26 November 2010, *http://www.ateneadigital.es/RevistaAtenea/REVISTA/articulos/GestionNoticias_3432_ESP.asp*. Both accessed 23 August 2012.

237 Inter-American Court of Human Rights, Demanda en el caso de Humberto Antonio Palamara Iribarne (Caso 11.571) contra la República de Chile, 13 April 2004.

238 Humberto Palamara, *Ética y servicios de inteligencia* (Valparaíso: Armada de Chile, 2006), pp. 65-66.

239 Giorgio del Vecchio, *Crisis del Derecho y Crisis del Estado* (Madrid, Librería General de Victoriano Suarez, 1935), p. 96.

240 Jose Luis Cea Egana, "Estado constitucional de derecho, nuevo paradigma jurídico," *Anuario de Derecho Constitucional Latinoamericano*, no. 11 (2005), pp. 47-50.

241 See Norberto Bobbio, *Estado, Gobierno y Sociedad: Por una Teoría General de la Política* (México DF: Fondo de Cultura Económica, 2006), pp. 68-187.

242 See Lucia Meza and Daniel Soto, "Seguridad, Derechos Humanos y Democracia: ¿Un Nuevo Paradigma?," *Revista IIDH, Instituto Interamericano de Derechos Humanos no*. 49 (2010), pp. 239-263.

243 Diego Torrente, *Desviación y Delito* (Madrid, Alianza Editorial, 2001), p. 223.

244 Fernando Velasco Fernandez, "Democracia y Servicios de Inteligencia: Ética para qué?," in Jose Luis Gonzalez Cussac, coord., *Inteligencia* (Valencia, Tirant Lo Blanch, 2012), p. 464.

245 *Ibid*., p. 474.

246 See Mark Riebling, *Wedge: The Secret War between the FBI and CIA* (New York: Alfred A. Knopf, 1994), pp. 121-125.

247 Jose Gonzalez Cussac, Beatriz Larriba Hinojar and Antonio Fernandez Hernandez, "Servicios de Inteligencia y Estado de Derecho," in Jose Luis Gonzalez Cussac, coord., *Inteligencia, op. cit*., pp. 283-287.

248 Florian Henckel von Donnersmarck, *La Vida de los Otros*, [DVD], Germany, Wiedermann and Berg Filmproduktion, Bayerischer Rundfunk, Arte y Creado Film, 2006.

249 Juan Jose Campanella, *El Secreto de Sus Ojos*, [DVD], Argentina, Tornasol Films, Haddock Film, 100 Bares, Telefe and others, 2009.

250 Joel and Ethan Coen, *Quémese Después de Leerse*, [DVD], United States, Bronx Community College, University Avenue at West 181 Street, Bronx, New York City and others, 2008.

251 Gregor Jordan, *El Dia del Juicio Final*, [DVD], United States, Lleju Productions and Films and Sidney Kimmel Entertainment International, 2009.

252 United Nations, *Derechos Humanos y Aplicación de la Ley: Manual de Capacitación en Derechos Humanos para Policía* (Geneva, High Commissioner for Human Rights, Center for Human Rights, 1997), pp. 59-66.

253 International Covenant on Civil and Political Rights (article 13.3) and American Convention (article 22.3).

254 Universal Declaration of Human Rights (article 20), International Covenant on Civil and Political Rights (article 20), American Declaration of the Rights and Duties of Man (article XXII), American Convention on Human Rights (article 16), International Covenant on Economic, Social and Cultural Rights (article 8), Covenant 87 on the Freedom of Association and the Protection of the Right to Organize (articles 2 through 5), Convention on the Rights of the Child (article 15), International Convention of the Protection of the Rights of All Migrant Workers and Members of their Families (articles 26 and 40).

255 Universal Declaration of Human Rights (articles 10 and 11), American Declaration of the Rights and Duties of Man (articles XVIII and XXVI), International Covenant of Civil and Political Rights (articles 14 and 15), American Convention on Human Rights (articles 8 and 9), Convention on the Rights of the Child (article 40) and Body of Principles for the Protection of All Persons Under Any Form of Detention or Imprisonment (principle 17).

256 William Friedkin, *Contacto en Francia*, [DVD], United States, D'Antoni Productions, Schine–Moore Productions, 1971.

257 Universal Declaration of Human Rights (articles 6 and 12), International Covenant on Civil and Political (articles 16, 17), American Declaration of the Rights and Duties of Man (articles V, IX, X, and XVII), American Convention on Human Rights (articles 3, 11, and 14), Convention on the Rights of the Child (article 16).

258 Adopted by the General Assembly of the United Nations in its Resolution 34/169 of 17 December 1979.

259 Universal Declaration of Human Rights (articles 10 and 11), American Declaration of the Rights and Duties of Man (articles XVIII and XXVI), International Covenant on Civil and Political Rights (articles 14 and 15), American Convention on Human Rights (articles 8 and 9).

260 United Nations, *op. cit.*, p. 63.

261 Martin Scorsese, *Los Infiltrados*, [DVD], United States, Warner Bros. Pictures, Plan B Entertainment, Initial Entertainment, 2006.

262 Universal Declaration of Human Rights (article 12), International Covenant for Civil and Political Rights (article 17), American Declaration of the Rights and Duties of Man (article IX), and American Convention on Human Rights (article 11).

263 Universal Declaration of Human Rights (article 11), American Declaration of the Rights and Duties of Man (article XXVI), International Covenant on Civil and Political Rights (article 14.2), American Convention on Human Rights.

264 Daniel O'Donnel, *Derecho Internacional de los Derechos Humanos: Normativa, Jurisprudencia y Doctrina de los Sistemas Universal e Interamericano* (Santiago, Regional Office for Latin America and the Caribbean, High Commissioner of the United Nations for Human Rights, 2007), p. 526.

265 Maria Eugenia Ullman et al., *Derechos Humanos, Seguridad Ciudadana y Funciones Policiales: Módulo instruccional* (San José, Instituto Interamericano de Derechos Humanos, 2011), pp. 85-89.

266 Paul Greengrass, *La Ciudad de las Tormentas*, [DVD], United States, Universal Pictures, Studio Canal and Relativity Media, 2010.

267 Universal Declaration of Human Rights (article 5); American Declaration of the Rights and Duties of Man (articles I, XXV, and XXVI); International Covenant of Civil and Political Rights (articles 7 and 10); American Convention on Human Rights (article 5); Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment; Inter-American Convention to Prevent and Punish Torture; Standard Minimum Rules for the Treatment of Prisoners; Body of Principles for the Protection of All Persons Subjected to Detention or Imprisoned; and United Nations Rules for the Protection of Juveniles Deprived of Their Liberty.

268 International Covenant for Civil and Political Rights (article 9.2) and American Convention on Human Rights (article 7.4).

269 American Declaration of the Rights and Duties of Man (article XXV paragraph 2), International Covenant for Civil and Political Rights (article 10), and American Convention on Human Rights (article 5 paragraph 2).

270 Gillo Pontecorvo, *La Batalla de Argel*, [DVD], Italy and Algeria, Igor Fil y Casbah Film, 1966.

271 Central Intelligence Agency, "Does the CIA Spy on Americans? Does It Keep a File on You?" *https://www.cia.gov/about-cia/faqs/index.html#spyonamericans*. Accessed 17 April 2011.

272 The Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment (1984) establishes in its article 1: "For the purposes of this Convention, we understand by the word 'torture' any act used to intentionally inflict pain, great suffering, whether physical or mental, on a person with the objective of obtaining from that person or a third person, information or a confession, in punishment for an act that person has committed, or is suspected of committing, or to intimidate or coerce this person or others, or for any reason based on any type of discrimination, when this pain and suffering are inflicted by a public official or other person in the exercise of public duties, on their own volition or with their consent and acquiescence. Any pain and suffering that is the result of legitimate sanctions, or that are inherent or incidental to those, will not be considered torture." The Inter-American Convention to Prevent and Punish Torture (1985) notes in its article 2: "For the purposes of this Convention, torture will be understood to be any act carried out intentionally that inflicts physical or mental pain or suffering for the purposes of criminal investigation, as a means of intimidation, as personal punishment, as a preventive measure, as a penalty, or for any other purpose. Also considered torture is the application of any method that tends to change the personality of the victim, or to diminish his or her physical or mental abilities, even though it may not cause physical pain or psychiatric anguish.… What will not be considered torture are physical or mental pain and suffering that are only the consequence of legal measures, or of practices inherent in those measures, so long as they do not include the actions or methods that are specifically noted in this article."

273 Pablo Bonorino asserts that liberalism rejects torture because of its close connection with tyranny and because it constitutes an extreme negation of human dignity. In applying such measures, the torturer crushes, terrorizes, and humiliates the victim for the purpose of dominating him or her through pain. This has been the objective of military victories, as a way to dominate politically through terror, as punishment, and as a procedure to extract confessions under an absolutist justice system. Pablo Bonorino Ramirez, "Retorno de la tortura: la carga ideológica de la ficción televisiva," *Revista Académica*, no. 51 (2011): pp. 111, 112.

274 Bonorino, *ibid*., pp. 109-215.

275 Humberto Antonio Palamara Iribarne sued the State of Chile because in 1993, while he was a civil employee of the navy, that institution prohibited him from publishing his book *Ethics and the Intelligence Services*. The unauthorized publication

of the book and his publicly declared disagreement with authorities, in defiance of the Naval Judge of Magallanes, brought on the confiscation of all copies of his book, the removal of the document from the hard disk of his computer, preventive imprisonment for 11 days, and the definitive judgment that his actions included "failure to perform military duties," "disobedience," and "disrespect." The Inter-American Court of Human Rights ruled against Chile and ordered the reform of its military justice system. (*Case of Palamara Iribarne vs. Chile*, 2005): Inter-American Court of Human Rights, 22 November 2005.

276 Humberto Antonio Palamara Iribarne, *Ética y Servicios de Inteligencia* (Valparaíso, Armada de Chile, 2006), p. 147.

277 Amalio Blanco Abarca, "La Condición de 'Enemigo': El Ocaso de la Inocencia," in Manuel Cancio Melia and Laura Pozuelo Perez, coords., *Política criminal en vanguardia: Inmigración clandestina, terrorismo, criminalidad organizada* (Navarra, Spain: Editorial Aranzadi SA, 2008), pp. 257, 258.

278 Henri Tajfel, *Human Groups and Social Categories: Studies in Social Psychology* (Cambridge: Cambridge University Press, 1981), p. 145.

279 Blanco Abarca, *op. cit.*, pp. 292, 293.

280 Amartya Sen, *Identity and Violence: The Illusion of Destiny* (New York: W. W. Norton & Company, 2007), pp. 1-8.

281 Younger-Yusuf reproaches his captors: "Do it! Do it! I love my country, you people crap on it! I love my religion, you people spit on it! Just remember something, I'm here because I wanna be here! I let myself be caught, because I'm not a coward! I chose to meet my oppressors face to face! You call me a barbarian? Then what are you? What, you expect me to weep over 50 civilians? You people kill that number every day! How does it feel Brody? This is not about me! This is about you! How does it feel? You have no authority here! None! There is but one authority, and it is not you! You are a blight, you are a cancer! How does it feel Brody?"

282 Sen, *op. cit.*, p. 175

283 Alias "H": "There is no H. and Younger ... there's only victory and defeat. The winner gets to take the moral high ground, because they get to write the history books. The loser ... just loses. The only miscalculation in your plan ... was me."

284 Albert Bandura, "Moral Disengagement in the Perpetration of Inhumanities," *Personality and Social Psychology Review*, 3, no. 3 (1999): p. 200.

285 See Bandura, *ibid*.

286 Jack Saunders, the Director of the FBI and Helen Brody's supervisor, shouts in desperation, "If those bombs go off there will be no f*#@ing Constitution!"

287 In November 2012, the Argentine Minister of Security, Sergio Berni, said, upon the capture of a presumed and infamous trafficker, "that as soon as the Argentine police forces discovered that Lopez Londono had entered the country toward the end of last year, they began an investigation to find his hideout." From *http://www.animalpolitico.com/2012/11/capturan-al-narco-mas-importante-del-mundo/*. Accessed 23 January 2014.

In Colombia, in November 2013, a former paramilitary official was captured, and the press chose to report that: "the police intelligence directorate said that his enjoyment of money, good food, and women were always his weaknesses." From *http://www.rpp.com.pe/2013-12-08-narcotraficante-colombiano-pantera-cayo-por-tener-tres-mujeres-noticia_653495.html*. Accessed 23 January 2014.

In 2011, the Mexican Minister of the Interior, Alejandro Poire, made it known to the press that "Operation Guest" had been put in place to detain Saadi Gaddafi, son of Muammar Gaddafi. The minister said, with respect to the operation, "the civilian intelligence services had detected an illegal plan for the infiltration of Saadi and his family into Mexico, and had proceeded in accordance with appropriate protocols and procedures." From *http://www.cronica.com.mx/notas/2012/620994.html*. Accessed 24 January 2014.

288 For those classical formulations, see the different versions of the *Libros Blancos de Defensa* of Latin American countries, www.resdal.org.

289 Governance has been operationalized as a concept to evaluate the behavior and evolution of democracies using indicators that reflect a country's adaptability and achievement of international norms. It is an expression of the institutional viability of a country. See *http://info.worldbank.org/governance/wgi/index.asp*.

290 See Jose Manuel Ugarte, "Las estructuras de inteligencia en América Latina," *Foreign Affairs en Español* (primavera 2002), p. 60; Carlos Maldonado, *Servicios de inteligencia en Sudamérica: Estado de situación en perspectiva comparada* (Fort Benning, Georgia: Instituto de Cooperación para la Seguridad Hemisférica–WHINSEC, June 2002).

291 See Russell G. Swenson and Susana C. Lemozy, *Profesionalismo de Inteligencia en las Américas/Intelligence Professionalism in the Americas* (Washington, DC: Joint Military Intelligence College, 2004).

292 The greatest requirements for international intelligence exchange lie in activities associated with organized crime, to include terrorism, narcotrafficking, and money laundering. This interaction involves officials who are directly responsible for the substance of the exchange, whether police, military, or others.

293 See, among others, Michael Hermann, *Intelligence Power in Peace and War* (Cambridge: Cambridge University press, 1996) and Richard K. Betts, *Enemies of Intelligence* (New York: Columbia University Press, 2007). The Sherman Kent Center for Intelligence Analysis also has produced several works of interest. For Latin America, see Thomas C. Bruneau and Steven C. Boraz, eds., *Reforming Intelligence: Obstacles to Democratic Control and Effectiveness* (Austin, Texas: University of Texas, 2007); Russell G. Swenson and Susana C. Lemozy, *Democratización de la función de inteligencia: El nexo de la cultura nacional y la inteligencia estratégica* (Washington, DC: National Defense Intelligence College, 2009); Jose Manuel Ugarte, *op. cit.*; Carlos Maldonado, *op. cit*.

294 Ohad Leslau, "The Effect of Intelligence on the Decisionmaking Process," *International Journal of Intelligence and Counterintelligence*, 23, no. 3 (2010), pp. 426-448.

295 Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little Brown, 1972).

296 See Yaacov Y.I. Vertzberger, "Bureaucratic-Organizational Politics and Information Processing in a Developing Country," *International Studies Quarterly* 28, no. 1 (1984), pp. 69-95.

297 The presidential advising arrangements for the United States, France and the United Kingdom tend to be set forth as successful examples where the products of intelligence systems are regularly incorporated. In Latin America, at the presidential level, the incorporation of the products of intelligence systems in decision making has not yet been worked out, and little literature exists on the topic. Some attention to the topic does appear in Deborah Stone, *Policy Paradox: The Art of Political Decisión Making*, revised edition (New York and London: Norton & Company, 2002); Michael Nelson, ed., *The Presidency and the Political System*, ninth edition (Washington, DC: CQ Press, 2010); and Michelangelo Vercesi, "Cabinets and Decision-Making Processes: Re-assessing the Literature," *Journal of Comparative Politics* 5, no. 2 (July 2012), *http://www.cpupi.si/assets/jcp/JCP-Issue-8-July-2012.pdf*. For some particulars about Chile, see Maria de los Angeles Fernandez and Eugenio Rivera Urrutia, eds., *La Trastienda del Gobierno* (Santiago de Chile: Catalonia, 2012). The establishment of presidential decisionmaking support structures

is an unfinished theme in the literature on the role and functions of intelligence systems in Latin America.

298 Strategic intelligence refers to the production of knowledge about themes and issues of vital national interest. It exists for the purpose of advising the highest political officials so as to anticipate, prevent, and resolve threats or risks to a democratic state.

299 Russell G. Swenson and Susana C. Lemozy, *Profesionalismo de inteligencia en las Américas/Intelligence Professionalism in the Americas, op. cit., and Democratización de la función de inteligencia/Democratization of Intelligence: Melding Strategic Intelligence* and *National Discourse, op. cit*.

300 See Nicolas Boscovich, "Pensamiento geopolítico brasileño," in *Geopolítica* (Buenos Aires), no. 34 (1986). Also see Lucas Figueiredo, *Ministério do silêncio* (Sao Paulo: Editora Record, 2005).

301 Especially the Argentine journal *Estrategia*, managed by General Juan E. Guglialmelli.

302 A good example is the Uruguayan intelligence law, still under consideration in the Uruguayan Congress. The defense law was approved toward the end of 2008.

303 See Carlos Reppalli, *Inteligencia criminal en el siglo XXI* (Buenos Aires: Lajouane, 2009). By the same author, *Inteligencia Criminal para la legislación de la Nación Argentina* (Buenos Aires: Lajouane, 2007). On economic intelligence, see Walter Felix Cardoso, Andrea Lodeiro, trans., *Guía de inteligencia empresarial: Enfrentando el ambiente de la alta competencia* (Buenos Aires: Seguridad y Defensa, 2006).

304 Thomas Bruneau, "Controlling Intelligence in New Democracies," *International Journal of Intelligence and Counterintelligence* 14:3 (Fall 2001), pp. 323-341.

305 Armando Borrero Mansilla has explained the logic of intelligence organizations that, with the consent of the government or not, avoid or ignore control mechanisms. According to this Colombian intellectual, if information is power, power provides security, and security increases the chances of one's survival, then transparency is not to be valued because it puts at risk the community that is to be defended. See Armando Borrero Mansilla, "De Wikileaks a la trivialidad y al olvido: Reir, llorar…o rezar," *Razón Pública*, 13 December 2010.

306 "Temen crisis institucional en Brasil por escuchas ilegales," *Infobae*, 1 September 2008.

307 "Hijo de puta, no vuelva a este país," *ABC* (*Madrid*), 28 September 2010.

308 "Cubanos realizan espionaje digital en Venezuela," *Infolatam*, 16 June 2011.

309 Véase "Los papeles secretos del DAS," *Semana.com*, 17 September 2011, *http://www.semana.com/nacion/papeles-secretos-del-das/164304-3.aspx*. Accessed 7 April 2012.

310 See Mariano Bartolome and Javier Ortiz, "Apuntes sobre la inteligencia en la Posguerra Fría," *Seguridad Estratégica Regional* (SER) no. 8 (1995), pp. 71-79. Also Mariano Bartolome, "El desafío de la inteligencia estratégica," *Informe de investigación* no. 1 (Buenos Aires: Instituto de Investigaciones sobre Seguridad y Crimen Organizado–ISCO, Universidad Católica de Salta, December 1999).

311 Marco Cepik, *Espionagem e Democracia* (Rio de Janeiro: Editora FGV, 2003), pp. 27-28.

312 Additional nuances exist in each of these areas. For example, in terms of "control" over intelligence by the legislative branch: Is it carried out by a single committee or commission, or by multiple ones? Is it a bicameral commission, or does it operate only in one legislative body? Is the commission created expressly for oversight, or has this task been assigned to a preexisting committee or commission, such as a defense committee? Do intelligence organizations have the obligation to present periodic reports to the commission, or only as they are specifically called for?

313 The Argentine case illustrates the dilemmas that can arise with respect to strategic intelligence: although the concept is employed as an accepted term of practice, Law 25520, which regulates intelligence activity, does not mention the term strategic intelligence, and the promulgation of this law implied the closure of the National Intelligence Center, which had carried out this specific responsibility.

314 The author knows of only one lengthy exchange on the topic of strategic intelligence among practitioners, congressional advisers, and academics involved in intelligence, its characteristics, and future challenges. This exchange occurred in a seminar titled "Strategic Intelligence in State Reform," which took place over much of 1992 in the Argentine National Intelligence School. The final report on the deliberations was published by the professional journal of that institution. See "La

Inteligencia Estratégica en la reformulación del Estado," *Revista de la ENI* 3, no. 1 (Buenos Aires, 1994), pp. 143-152.

315 From a constructionist perspective, "securitization" is a political discourse process through which a political community decides to deal with a phenomenon such as a threat by making it a valued referent, setting the stage for the adoption of time-sensitive steps to reduce the threat.

316 Angel Tello, "La incertidumbre estratégica," in Mariano Bartolome, comp., *Seguridad y defensa en tiempos de bicentenario: Visiones desde Argentina y Chile* (Buenos Aires: Instituto de Publicaciones Navales, 2010), pp. 21-34; Natalie Pabon Ayala, "Las relaciones cívico-militares en la política de seguridad democrática," in Alejo Vargas Velasques. ed., *Perspectivas actuales de la seguridad y la defensa en Colombia y América Latina*, Colección Gerardo Molina no. 15 (Bogota: Universidad Nacional de Rosario, 2008), pp. 51-64.

317 "Senderistas se capitalizan en Bolivia," *La Razón*, 7 March 2009; "Cómo funciona el mayor centro de venta de drogas," *Clarín*, 18 April 2010.

318 The author considers the reports released by the government of Colombia concerning the information contained on the personal computers of Raul Reyes to be accurate, and accepts the verification of that information by INTERPOL, which has made the details a matter of public record. See OIPC-INTERPOL, *Informe forense de Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados por Colombia* (Lyon: OIPC-INTERPOL, 2008).

319 Mariano Bartolome, "Secuestros extorsivos y reivindicaciones campesinas: la rara alquimia del Ejército Popular Paraguayo," *Analítica*, 5 May 2010, *http://www.analitica.com/va/internacionales/opinion/3857731.asp*. Accessed 11 April 2012.

320 Figures released in July 2009 by the Secretary General of this organization, Miguel Insulza, in his presentation to the Inter-American Conference on Public Security in Montevideo, Uruguay. See Mariano Bartolome, "Situación del Crimen Organizado en América Latina," *Ágora Internacional*, no. 10, (November 2009), pp. 16-20.

321 The report also indicates Mexico hosts five of the ten most violent cities of the world; the Americas count 45 of the 50 most violent cities, with 40 of those in Latin America. For more information, see *Consejo Ciudadano para la seguridad pública y la justicia penal: Metodología del ranking (2011) de las 50 ciudades y las 50 jurisdicciones subnacionales más violentas del mundo* (México DF, 12 January 2012).

322 United Nations Office on Drugs and Crime, *World Drug Report* (Vienna: UNODC, 2011), pp. 85-126.

323 Mariano Bartolome, "Colombia: Bandas Criminales (BACRIM)," *Reconciliando Mundos*, no. 7, (September-October 2011), pp. 16-22.

324 Rachel Stohl and Doug Tuttle, "The Small Arms Trade in Latin America," *NACLA Report on the Americas* 41, no. 2 (March-April 2008), p. 14. Also see Fernando Gualdoni and Javier Lafuente, "Las armas ilegales desangran Latinoamérica," *El País*, 25 May 2009.

325 "Tráfico de armas en los Andes," *El Universal*, 27 April 2008.

326 Grupo de Estudiantes de Relaciones Internacionales de la Universidad de Palermo (GERIUP), "Tráfico de personas en América del Sur," *Informes del GERIUP*, 19 October 2011.

327 On this point, the preventive idea is of fundamental importance. A report of the International Bank for Development (BID) (see *http://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=876738*) finds that adequate investment in prevention reduces between six and seven times the investment that would need to be made after the crimes are carried out. See Jorge Serrano Torres, *Las potencialidades de una doctrina y un sistema de inteligencia criminal para desarticular al crimen organizado y afianzar la seguridad ciudadana en el Perú* (Lima: Projusticia-Centro de Estudios para el Desarrollo de la Justicia, November 2011). The present author considers that the reduction of costs that come from prevention of terrorism yields an even greater savings.

328 Carlos Gutierrez Palacios, "El papel de la inteligencia estratégica ante los desafíos regionales," *Revista Atenea*, 6 October 2010.

329 "Narcotráfico debe verse como una amenaza para toda la región, dijo el jefe de inteligencia brasileña," *El Tiempo*, 13 August 2009.

330 "Forman a militares para combatir al EP," *ABC Color*, 1 March 2011; "Defensa tendrá más poder sobre las Fuerzas Armadas, reconoce el ministro," *ABC Color*, 3 March 2011.

331 "Claves de la reforma de las Fuerzas Armadas," *La República*, 7 March 2011.

332 "Video: Colman (DNII) duda de la existencia de un ejército paralelo," *La Red 21*, 17 March 2011.

333 See Luis Casal Beck, "Una inteligencia segmentada," *La Red 21*, 1 April 2011.

334 "El DAS deja de existir para dar paso a la Agencia Nacional de Inteligencia, *Semana.com*, 31 October 2011. For a good summary of the period leading up to the dissolution of the DAS, the different bills presented in Congress to put in place an organization replacing the DAS, and other related questions, see "Agencia Central de Inteligencia de Colombia," *Observatorio Legislativo del Instituto de Ciencia Política*, Boletín no. 144 (November 2009).

335 Serrano Torres, *op. cit.*

336 See details about this operation in "Así cayó Raúl Reyes," *Cambio*, 12 March 2008.

337 Maria Amparo Tortosa Garrigos, "Cómo se están redefiniendo las agencias de inteligencia: Las nuevas amenazas y conflictos requieren de un nuevo tipo de cooperación," *Safe Democracy*, 12 January 2009.

338 Roger Zane George, "Beyond Analytic Tradecraft," *International Journal of Intelligence and CounterIntelligence* 23, no. 2 (June 2010).

339 Chilean specialist Carolina Sancho Hirane suggests a useful distinction between an intelligence system and an intelligence community. Whereas a *system* depends on regular interaction or dependency among its intelligence organizations, a *community* involves diverse, public organizations that each have a separate, substantive, and systematic role to fulfill with respect to the state's strategic interests. See Carolina Sancho Hirane, "Servicios de Inteligencia en las Américas: Estado del debate y desafíos pendientes," in Mariano Bartolome, comp., *Seguridad y defensa en tiempos de bicentenario: Visiones desde Argentina y Chile* (Buenos Aires: Instituto de Publicaciones Navales, 2010), pp. 149-168.

340 "Mujica no aceptó la renuncia de Grégori, el Coordinador Nacional de Inteligencia," *La Red 21*, 1 April 2011.

341 "Comando conjunto de fuerzas armadas asumió control del Sistema de Inteligencia," *El Universo*, 18 Ocrober 2010.

342 "Colombia: Santos crea la figura del Consejero de Seguridad Nacional," *Infolatam*, 20 September 2010.

343 United Nations Organization, *Un mundo más seguro: la responsabilidad que compartimos. Informe del Grupo de Alto Nivel sobre las amenazas, los desafíos y el*

cambio, A/59/565, 2 December 2004, *http://www.un.org/spanish/secureworld/report_sp.pdf*. Accessed 7 April 2012.

344 Felix Arteaga, "Una década de cambios en la seguridad tras el 11-S: de la globalización a la glocalización," *Real Instituto Elcano, ARI* 125/2011, 6 September 2011.

345 "Sendero Luminoso es hoy un museo de cera del terrorismo que había en el Perú," *El Comercio*, 7 September 2010.

346 "Zares antidrogas buscan combatir lavado de activos del narcotráfico," *El Nuevo Herald*, 5 October 2010.

347 Mario Baizán, "Cooperación internacional en la zona de la Triple Frontera," *mimeo* (Buenos Aires: Fundación de Estudios Políticos para el Tercer Milenio -FUPOMI, 2004), *http://www.fupomi.com.ar/img/TripleF.pdf*. Accessed 7 April 2012.

348 Publicly available information on these units is scarce, especially of an academic nature. Among the few available sources is Ramon Quiroga, "Políticas de Seguridad y Defensa en América del Sur," paper presented at the Fifth Conference of National Strategic Studies, Buenos Aires, October 2002.

349 Felix Arteaga, "Una década de cambios en la seguridad tras el 11-S: de la globalización a la glocalización," *Real Instituto Elcano, ARI* 125/2011, 6 September 2011.

350 Pablo Martinez, *Triple Frontera: un modelo de cooperación antiterrorista* (Montevideo: Centro de Estudios Hemisféricos de Defensa (CHDS), Conferencia Subregional de Defensa "Seguridad Transnacional y Gobernabilidad," November 2005).

351 The Latin American and Caribbean Police Intelligence Community was created in 2005, with the objective of promoting intelligence personnel career development and fomenting interaction among members. Today members are from 30 countries, with external observers from the United Nations, the Organization of American States, EUROPOL, and Spain's National Intelligence Center (CNI).

352 "México compartirá su plataforma de inteligencia con América Latina y el Caribe," *Agencia EFE*, 3 July 2010.

353 One may understand by "scenario" the concept employed by the Saint Gall Center for Futures Research: "images of the future that represent a process, are based on a methodology, incorporate the knowledge of experts and that facilitate organizational learning."

354 Richard Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington, DC: National Defense University Press, 2006), pp. 37-38.

355 Some of the numerous references to this mode of strategic analysis: Bjørn Moller, "Ethnic Conflict and Postmodern Warfare: What Is the Problem? What Could Be Done?," COPRI, Working Paper, October 1996; Eric de la *Maissonave, Incitation à la Reflexion Stratégique* (Paris: Economica, 1998); Alain Joxe, *El Imperio del Caos* (Buenos Aires: Fondo de Cultura Económica, 2003); and U.S. Army, *Counterinsurgency Field Manual* (Chicago: The University of Chicago Press, 2007).

356 The use of historical analogies can be valid for contemporary international political analyses, such as in strategic intelligence. However, the perspective that insists that every contemporary international phenomenon, without exception, is equally well understood through some historical referent, is not correct. This point is developed by Robert Kaplan, in *El retorno de la antigüedad: La política de los guerreros* [The Return of Ancient Times] (Barcelona: Editorial B, 2002).

357 "Colombia ya cuenta con un nuevo material estadístico del Sector de la defensa y la seguridad," *Infodefensa.com*, 7 September 2010.

358 George Friedman, *The Next 100 Years. A Forecast for the 21st Century* (New York: Anchor Books, 2010).

359 National Intelligence Council, *Global Trends 2015: A Transformed World* (Washington, DC: U.S. Government Printing Office, November 2008).

360 Jose Miguel Pizarro, "América Latina: la guerra que ya no podemos evitar," *Revista AAInteligencia* 2010-3, *http://www.aainteligencia.cl*.

361 Rogelio Nunez, "Sendero Luminoso: de guerra maoísta a cártel," *Revista Atenea*, 14 February 2011.

362 The CDS is the regional security council for the 12 countries of the Union of South American Nations (UNASUR). It emerged in the wake of the crisis brought on by the Colombian attack on the FARC encampment in Ecuadorian territory in March of 2008. The council was created in Santiago, Chile, in March of 2009 through the "Declaration of Santiago de Chile." The 12 countries agreed to build a uniquely South American identity to handle security challenges and contribute to the strengthening of Latin American and Caribbean unity.

363 The author wishes to thank Andres Gonzalez Vargas, professor at the *Universidad Jorge Tadeo Lozano*, Bogota, for the artwork in this essay, and gratefully acknowledges the support of the author's wife, Amparo Vasquez Gallo.

364 Gregory Treverton, "Intelligence and the 'Market State,'" *Studies in Intelligence* 10 (Winter/Spring 2001), p. 71.

365 Carlos Lleras Restrepo, "Los escándalos financieros," *Revista Nueva Frontera*, Bogota (July 1988).

366 See Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats Are Hijacking the Global Economy* (New York: Doubleday, 2005).

367 Pilar Pozo Serrano, "Externalización de funciones de inteligencia: oportunidades y riesgos a la luz de la experiencia estadounidense," *Inteligencia y Seguridad: Revista de análisis y prospectiva*, no. 6 (June-November 2009), p 19, *http://api.ning.com/files/0M9hu7HM12wNGdreMNlIP8gF6Rn2U-fJSMXBIjf9b*3ttSwCtlxK6sVGf-iUq2ugpZva7LNBoUi1En8XjSY-QZ9clfviV1sL/inteligenciaprivada.pdf*. Accessed 28 September 2011.

368 Congreso de Colombia—Decreto Ley 599 de 2000 (Código Penal), Title XVII, Chapter II, Article 463 (on crimes against the security of the state): "Espionage: To improperly obtain, employ or reveal political, economic or military secrets related to the security of the state, will incur from four to twelve years imprisonment."

369 Percy García Cavero, *Derecho Penal Económico*, vol. I (Lima: Editorial Jurídica Grijley, 2007), pp. 103 and 105.

370 Agencia Venezolana de Noticias, 20 July 2010, *http://www.avn.info.ve/node/5988*. Accessed 27 August 2012.

371 See Eldiario.ec, 18 February 2010, *http://www.eldiario.com.ec/noticias-manabi-ecuador/144026-incluyen-a-ecuador-en-lista-negra-de-lavado-de-dinero/*. Also, Patricio X. Sanchez, Ramiro Crespo Fabara, and Patricio Starnfeld Llamazares, "Prevención de lavado de activos frente a la concienciación: Conferencia sobre lavado de activos y financiamiento del terrorismo," in *Inteligencia Estratégica y Prospectiva*, Fredy Rivera Vélez, coord. (FLACSO, Quito, Ecuador, and Secretaría Nacional de Inteligencia del Ecuador, 2011), pp. 239-64.

372 Andres Montero Gomez and Jose Martin Ramirez, "Inteligencia económica como vector internacional de seguridad," *Real Instituto Elcano*, 21 April 2008, *http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/dt18-2008.* Accessed 8 January 2011.

373 Ohad Leslau, "Intelligence and Economics: Two Disciplines with a Common Dilemma," *International Journal of Intelligence and CounterIntelligence* 20, no. 1 (2007), p. 106.

374 Marco Palacios, "Saber es poder: el caso de los economistas colombianos," *De populistas, mandarines y violencias, luchas por el poder* (Bogotá, Editorial Planeta, 2001), pp. 119 and 134.

375 Jennifer Sims, "Defending Adaptive Realism: *Intelligence Theory Comes of Age," in Intelligence Theory: Key Questions and Debates*, Peter Gill, Stephen Marrin, Mark Phythian, eds. (London & New York: Routledge, 2009), p. 154.

376 Sims, *ibid*., p. 154.

377 "Refinería de Cartagena y ducto serían viables," *Petróleo y Gas*, 8 November 2005, *http://www.bnamericas.com/news/petroleoygas/Refineria_de_Cartagena_y_ducto_serian_viables*. Accessed 28 September 2011.

378 "As Rubens Ferreira de Mello notes in his *Tratado de Derecho Diplomático* [Discourse on Diplomatic Law]: Among the accusations made about diplomacy, one of the most common is that having to do with its history, not always admissible, of unscrupulous service to governments in terms of saving face and [maintaining] hegemony. This business is known as 'secret diplomacy' …. Certainly, face-saving and hegemonic intentions remain alive in executive branch offices where foreign policy is handled, and is not infrequently intentionally directed by those in power." See Diego Uribe Vargas, *Colombia y la diplomacia secreta* (Bogotá, Universidad Jorge Tadeo Lozano y Academia Colombiana de Historia, 2005), pp. 28 and 29.

379 "Inversiones de Chávez en el país son peligrosas: ex ministro Santos," *El Colombiano.com*, 8 November 2005, *http://www.elcolombiano.com/BancoConocimiento/O/olac_santos_se_refiere_a_interes_de_chavez_colprensa_lcg_08112005/olac_santos_se_refiere_a_interes_de_chavez_colprensa_lcg_08112005.asp.* Accessed 12 December 2010.

380 Claudia Curiel Leidenz, "La economía durante la Revolución Bolivariana," *Hugo Chávez: Una década en el poder* (Bogotá, Centro de estudios Políticos e Internacionales, Universidad del Rosario, 2010), p. 414.

381 Moisés Naím, *Illicit, op. cit.*, p. 55.

382 *Ibid.*, p. 24.

383 Vanda Felbab-Brown, *Las economías ilegales y el contrabando en Colombia: Los señores de las moscas* (Washington, DC: Brookings Institution, 21st Century Defense Initiative, 22 February 2011), *http://www.brookings.edu/opinions/2011/0222_colombia_felbabbrown.aspx?sc_lang=es*. Accessed 28 September 2011. [Material in brackets added by author].

384 Cited in William J. Bernstein, *A Splendid Exchange, How Trade Shaped the World* (New York: Atlantic Monthly Press, 2008), p. 376.

385 Nonetheless, "There are several reasons why the armed forces of Venezuela are not as eager as Chávez to be confrontational. One reason is that the armed forces are major beneficiaries of licit and illicit commerce with Colombia and the United States." Javier Corrales, "Cambios en el tipo de régimen y la nueva política exterior de Venezuela", in *Hugo Chávez: Una década en el poder* (Bogota: Universidad del Rosario, 2010), p. 477.

386 This assertion is based on the author's professional experience.

387 Sims, *op. cit.*, p. 62.

388 Presidential address of 17 November 2008, *http://web.presidencia.gov.co/boletin/boletin_no2_17112008.html*. Accessed 5 March 2009.

389 "Las Farc también 'invirtieron' en DMG," *Revista Semana*, 19 February 2010, *http://www.semana.com/nacion/farc-tambien-invirtieron-dmg/135207-3.aspx*. Accessed 22 September 2011.

390 "Gobernador de Putumayo: las Farc estarían aprovechando crisis por las pirámides para poner al pueblo contra el gobierno," Radio Caracol, 2 December 2008, *http://www.caracol.com.co/nota.aspx?id=722564*. Accessed 5 March 2009.

391 "A responder por pirámides," El Espectador.com, 24 November 2008, *http://www.elespectador.com/impreso/articuloimpreso93236-responder-piramides*. Accessed 5 March 2009.

392 "En el caso de las pirámides, 'faltó gobierno,'" *El Espectador.com*, 15 November 2008, *http://m.elespectador.com/impreso/cuadernilloa/entrevista-de-cecilia-orozco/articuloimpreso90777-el-caso-de-piramides-falto-go*. Accessed 5 March 2009.

393 "¿Quién espía en Colombia?" Informe especial, *Semana.com*, 21 July 2003, *http://www.semana.com/nacion/quien-espia-colombia/71742-3.aspx*. Accessed 18 November 2010.

394 "Las revelaciones de Tabares y Peñate," *El Espectador.com*, 1 January 2011, *http://www.elespectador.com/impreso/judicial/articulo-242994-revelaciones-de-tabares-y-penate*. Accessed 18 January 2011.

395 Extrapolated from Sims, *Defending Adaptive Realism, op. cit*., p.156.

396 "In the case of Colombian exporters, when Chávez closed the border to commerce in mid-2009, the Venezuelans owed US$900 million. The border closure was accompanied by another, equally hostile act: refusal to allow payments for exports already in the hands of Venezuelans," *http://lanota.com/index.php/CONFIDENCIAS/Venezuela-no-le-paga-a-los-exportadores-colombianos.html*. Accessed 9 December 2011.

397 "A letter sent by the president of ANDI, Luis Carlos Villegas, to the then-president of Fedecamaras, and to Pedro Carmonas, for a few hours President of Venezuela, became a bone of contention between the government of Hugo Chávez and some elements of the Colombian business community." See "Empresarios descontentos," *El Tiempo*, 8 July 2003, *http://www.eltiempo.com/archivo/documento/MAM-1014926*. Accessed 5 June 2011.

398 "The government [of Ecuador] argues that a 40 percent devaluation of the Colombian peso existed at the time," while, according to data held by the Ecuadorian-Colombian Chamber of Commerce, "technically, the devaluation did not exist," per the Chamber's president, Milton Delgado. See "Ecuador pone en vigencia 'salvaguardia cambiaria' contra Colombia," Peopledaily.com, *http://spanish.peopledaily.com.cn/31617/6699818.html*. Accessed 12 January 2012.

399 Alphonso Chardy, "Chavez Expanding Influence of Cuban Advisers," *Miami Herald*, 8 May 2004.

400 "La tenaza cubana," *Semana.com* 13 February 2010, *http://www.semana.com/mundo/tenaza-cubana/134903-3.aspx*. Accessed 12 January 2012.

401 "Un pueblo sin memoria y malagradecido," *Eluniversal.com* (Caracas), 18 June 2011, *http://www.eluniversal.com/2011/06/18/un-pueblo-sin-memoria-y-malagradecido.shtml*. Accessed 13 September 2011.

402 "Juego de espías," *Semana.com*, 25 August 2007, *http://www.semana.com/nacion/juego-espias/105816-3.aspx*. Accessed 3 September 2011.

403 "El chavismo estaría financiando políticos en el territorio nacional. Renuncias en Monómeros por supuesta actividad chavista en Colombia," *El Espectador.com*, 14 August 2008, *http://www.elespectador.com/impreso/politica/articuloimpreso-renuncias-monomeros-supuesta-actividad-chavista-colombia*. Accessed 25 September 2011.

404 Sergeant Evelio Buitrago Salazar, *Zarpazo the Bandit: Memoirs of an Undercover Agent of the Colombian Army*, M. Murray Lasley, trans., Russell W. Ramsey, ed. (Tuscaloosa: The University of Alabama Press, 1977).

405 National Constitution, article 2: "These are the purposes of the State: to serve the community, promote the general prosperity and guarantee the application of sacred principles, rights, and obligations of the Constitution; facilitate the participation of everyone in the decisions that affect them individually and in the economic, political, administrative and cultural life of the nation; defend the nation's independence, maintain its territorial integrity and ensure the peaceful coexistence and maintenance of a just society. The authorities of the Republic are put in place to protect all people resident in Colombia, to include their life, honor, possessions, beliefs, and other rights and freedoms, and to ensure the accomplishment of social obligations to the State and to individuals."

406 "EE.UU. asume la protección del petroleo colombiano," *El Clarín*, 11 February 2002, *http://edant.clarin.com/diario/2002/02/11/i-02415.htm*. Accessed 28 September 2011.

407 See *http://www.egmontgroup.org/*.

408 Unidad de Información y Análisis Financiero, República de Colombia, Descripción de cargos, funciones y perfiles, no date, *http://www.uiaf.gov.co/index.php?idcategoria=677*. Accessed 13 August 2011.

409 Proyecto de Ley Estatutaria No. 195 de 2011. Artículo 3.—Agencies that carry out the function of intelligence and counterintelligence: The intelligence and counterintelligence function is carried out by elements of the armed forces and of the

national police, as organized for that purpose by the latter, the financial information and analysis unit (UIAF), and by other agencies as authorized by the law. These agencies make up the intelligence community and are the only entities authorized to develop intelligence and counterintelligence activities. All the agencies that carry out these activities will be entirely subject to the present law.

410 "Política de Consolidación de la Seguridad Democrática: Fortalecimiento de las Capacidades del Sector Defensa y Seguridad."

411 National Constitution, article 339. "There will be a National Development Plan that includes a general part and an investment plan for public entities at the national level. The general part will list long-term national purposes and objectives, the State's medium-term goals and priorities and the strategies and general aims of economic, social and environmental policies as adopted by the Government…."

412 Clara Elvira Ospina, ¿Inteligencia o intimidad? *Revista Poder360*, 18 September 2010, *http://www.poder360.com/article_detail.php?id_article=4755*. Accessed 12 February 2011.

413 Such as the steps taken by the U.S., as documented by Allain Juilet in "Principios y Aplicación de la Inteligencia Económica," *Inteligencia y seguridad: Revista de análisis y prospectiva*, no.1 (December 2006), p. 15, *http://www.intelligence-economique.gouv.fr/IMG/pdf/Article_Alain_Juillet_pour_revue_espagnole.pdf.* Accessed 30 May 2011.

414 According to Naim, *Illicit, op. cit*., p. 55, international terrorism, as we are beginning to realize, is following the path of worldwide illicit commerce by using the instruments and services of the new global economy to cover, and thereby hide, its activities in cities and whole countries.

415 Edward Luttwak, "From Geo-Politics to Geo-Economics," *The National Interest* 20, no. 3 (Summer 1990), p. 17.

416 Nicolás Urrutia, "Colombia necesita espías," *Semana.com*, 11 March 2009, *http://www.semana.com/opinion/colombia-necesita-espias/121626-3.aspx*. Accessed 11 June 2009.

417 Marta Ardila, *Actores no Gubernamentales y Política Exterior* (Bogotá, Centro de Estudios Internacionales, Universidad de los Andes, 2009), p. 115.

418 Douglas Farah, *Transnational Organized Crime, Terrorism and Criminalized States in Latin America: An Emerging Tier-One National Security Priority* (Carlisle, Pennsylvania: Strategic Studies Institute, U.S. Army War College, August 2012).

419 See White House, *National Security Council, Strategy to Combat Transnational Organized Crime*, part I, Definition, *http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/definition*. Accessed 16 February 2013.

420 *Ibid.*, part III, Strategy to Combat Transnational Organized Crime, *http://www.whitehouse.gov/administration/eop/nsc/transnational-crime/strategy.* Accessed 16 February 2013.

421 See the document at *http://www.mindef.mil.gt/ftierra/emdn/sage/directivas/documentos/leyesyreglamentos/04.pdf*. Accessed 16 February 2013.

422 Ley Marco del Sistema Nacional de Seguridad, Decreto No. 18-2008, approved by the Guatemalan Congress, 11 March 2008, Article 3, *http://www.mindef.mil.gt/noticias/PDF/leyes%20y%20reglamentos/Ley%20Marco%20%20D018-2008.pdf*. Accessed 16 February 2013.

423 The purpose of the national security system is to fortify state institutions, manage risks, control threats, and reduce vulnerabilities that inhibit the state's ability to accomplish its objectives. The national intelligence system encompasses the Secretary of Strategic Intelligence, who coordinates the system, the Office of Civilian Intelligence of the Interior Ministry, and the Intelligence Office of the General Staff for National Defense of the Ministry of Defense. See articles 4 and 24 of the *Ley Marco del Sistema Nacional de Seguridad Decreto* No. 18-2008, approved by the Congress of the Republic, 11 March 2008.

424 Technical secretary of the National Security Council, *Extracto Política Nacional de Seguridad de Guatemala*, Introduction (Guatemala: Mayaprin, 2012), p. 1.

425 The Advisory and Planning Commission was created to support the National Security Council. It operates in league with the technical secretary of the council. It is made up of security professionals who are appointed by the president of the republic upon the recommendation of Security Council members. See *Ley Marco del Sistema Nacional de Seguridad*, artículo 13, *http://www.mindef.mil.gt/noticias/PDF/leyes%20y%20reglamentos/Ley%20Marco%20%20D018-2008.pdf*.

426 Government of Guatemala, technical secretary of the National Security Council, *Política Nacional de Seguridad* (July 2012), pp. 28 and 36, *http://www.asies.org.gt/sites/default/files/articulos/publicaciones/5._anexo_i.3_politica_nacional_de_seguridad.pdf*. Accessed 15 February 2013.

427 See *http://www.mingob.gob.gt.previewdns.com/index.php?option=com_k2&view=item&id=1943:acuerdo-gubernativo-no-285-2012-protocolo-de-actuación-interinstitu-*

cional-apoyo-del-ejército-a-las-fuerzas-de-seguridad-civil&Itemid=394. This protocol signals that the president of the republic will decide when it is appropriate for the military to support civilian security forces inside the country. Earlier, Congressional Decree 40-2000 established, in its article 1, that civilian security forces may be supported in carrying out their functions of preventing and combating organized crime and common criminality by Guatemalan Army units as necessary when the country's circumstances require it and the "usual means employed by the civilian security forces are judged to be insufficient." *http://www.mindef.mil.gt/ftierra/emdn/sage/directivas/documentos/leyesyreglamentos/09.pdf*. Accessed 16 February 2013.

428 Decreto 11-97, *Ley de la Policía Nacional Civil*, artículo 9, 25 February 1997. See *http://www.oas.org/juridico/mla/sp/gtm/sp_gtm-mla-leg-police.pdf*. Accessed 25 February 2013.

429 "Se pone en marcha reforma policial", *politicagt.com*, 28 January 2010, *http://www.politicagt.com/se-pone-en-marcha-reforma-policial/*. Also see International Crisis Group, *Reforma policial en Guatemala: Obstáculos y oportunidades*, 20 July 2012, pp. 9-11. Both accessed 26 February 2013.

430 Dinorah Azpuru, *Cultura política de la democracia en Guatemala: Hacia la igualdad de oportunidades* (Wichita, Kansas: Wichita State University, December 2012), p. 151, *http://www.asies.org.gt/sites/default/files/articulos/publicaciones/guatemala_country_report_2012_vf_print_w.pdf*. Accessed 26 February 2013.

431 Comisión presidencial para la reforma policial, *Proyecto de implementación de la fase inicial de la reforma policial*, Producto 1 (Programa de las Naciones Unidas para el Desarrollo-Guatemala, Consultoría Análisis y Diseño de la Carrera Policial, March 2012). See *http://www.cnrp.gob.gt/content/acciones-prioritarias*. Accessed 11 March 2013.

432 Comisión presidencial para la reforma policial, *http://www.cnrp.gob.gt/content/ejes-verticales*. Accessed 13 March 2013.

433 Army of Guatemala, General Staff of National Defense, *Manual de asuntos civiles ME-20-02*. Authorized by the Chief of the General Staff of National Defense, December 2011.

434 Rodolfo Felipe Robles Montoya, *Propuesta de un Sistema de Inteligencia Nacional para Guatemala*, Chapter I, "Nociones básicas de inteligencia" (Guatemala: Fundación Myrna Mack and Fundación Soros, June 2003), p. 30.

435 Ulises Noe Anzueto Giron, Ministro de Defensa de Guatemala, personal communication with the authors, 11 March 2013.

436 *Ibid*.

437 Official web page of the Ministry of National Defense of Guatemala: *www.mindef.mil.gt*.

438 Acuerdo Gubernativo Número 153-2012, article 52, chapter VIII.

439 Carlos Manoel Alvarez Morales, "Se desgasta credibilidad del Gobierno: Analistas señalan que la sociedad está polarizada en temas de conflictividad," *Siglo21.com.gt*, 10 December 2012. As Edmundo Urrutia, of the Faculty of Latin American Social Sciences (Flacso), notes here, "What happened at Totonicapán is a manifestation of the weak capability of the system for processing the needs and demands of the indigenous peoples. The government and members of society should see this as an opportunity for discussion at a high level." *http://www.s21.com.gt/nacionales/2012/10/12/se-desgasta-credibilidad-gobierno*. Accessed 19 February 2013.

440 See Patrick Blankenship, "Out of the Andean Ridge," *Special Warfare* (October 2012). Reproduced at *http://www.soc.mil/swcs/SWmag/archive/SW2504/SW2504OutOfTheAndeanRidge.html*. Accessed 16 February 2013.

441 John P. Sullivan and Adam Elkus, "Policy and Strategy in the New Drug War," *Small Wars Journal* (24 October 2012), *http://smallwarsjournal.com/jrnl/art/policy-and-strategy-in-the-new-drug-war*. Accessed 15 February 2013.

442 Patrick Blankenship, *op. cit*.

443 Lieutenant Colonel Jeffrey A. Jacobs, U.S. Army Reserve, "Los asuntos civiles en las operaciones de paz", *Military Review* (January-February 1999), *http://usacac.army.mil/CAC2/MilitaryReview/Archives/oldsite/Spanish/JanFeb99/jacobs.pdf*. Accessed 8 March 2013.

444 "Defensa: El narcotráfico representa hechos aislados que no confrontan directamente al Estado," *Diario La Hora*, 7 May 2012, *http://www.lahora.com.gt/index.php/nacional/guatemala/reportajes-y-entrevistas/157905-defensa-las-manifestaciones-del-narcotrafico-son-hechos-aislados-que-no-confrontan-directamente-al-estado*. Accessed 11 March 2013.

445 The Municipal Development Councils are made up of the town or city mayor, who is also the individual charged with coordination within the council, trustees

and advisers as designated by the municipality, the representatives (up to 20) of the Community Development Councils, representatives of the public entities that are present in the locality, and the representatives of other local, civilian organizations as designated. The Community Development Councils encourage public participation in local planning and development and in local public administration. These Councils are part of the official System of Development Councils that operate at the national level.

446 Jennifer Schirmer, "Asuntos civiles: Guerra psicológica, inteligencia social y el maya autorizado," chapter 5 of the book *Intimidades del proyecto político de los militares en Guatemala* (Ciudad de Guatemala: Flacso, 2001), p. 179, *http://www.enlaceacademico.org/fileadmin/usuarios/mas_documentos/Lib057.pdf*. Accessed 15 February 2013.

447 The original document was sent by the authors to the Minister of National Defense, General de División, Ulises Noé Anzueto Girón, for his attention.

448 "Ejes de transformación y lineamientos estratégicos," chapter V of Gobierno de Guatemala, *Política Nacional de Seguridad*, 2012, p. 25.

449 Martin Nowak, Supercooperadores (Spain: Grupo Zeta, 2012), p. 55.

450 Sonia Alda and Héctor Saint-Pierre, coords., *Gobernabilidad y democracia* (Chile: RIL/UNESP/IUGM, 2012), p. 219.

451 All sovereign countries on the South American continent hold membership in UNASUR.

452 The present study is a part of a larger research project developed by the author for the Chilean *Academia Nacional de Estudios Politicos y Estrategicos* (ANEPE), under project Ext/12/2012, titled "Intelligence Cooperation and UNASUR: Possibilities and Limitations." The author wishes to thank political scientist Jean Gutierrez for her assistance.

453 Julia Pulido, "El papel de la inteligencia en la PESD [Política Europea de Seguridad y Defensa]", *Cuadernos de Estrategia* (Spanish Ministry of Defense) no. 130, 2005; Robert Clark, *Intelligence Analysis*, second edition (Washington, DC: CQ Press, 2007); Antonio Diaz Fernandez, coord., Miguel Revenga and Oscar Jaime, *Cooperación Europea en Inteligencia* (Spain: Thomson Reuters and IUGM, 2009).

454 Mathieu Deflem, "Global Rule of Law or Global Rule of Law Enforcement? International Police Cooperation and Counterterrorism," *Annals of the American*

Academy of Political and Social Science 603, Law, Society, and Democracy: Comparative Perspectives (January 2006), pp. 240-251.

455 Rhodri Jeffreys-Jones, *Historia de los Servicios Secretos Norteamericanos* (Spain: Editorial Paidos, 2004), p. 32.

456 Inge Kaul et al., *Bienes Públicos Mundiales* (Mexico: Oxford, 2001).

457 Peter Bergen and Alec Reynolds, "De nuevo, la contraofensiva a las acciones occidentales," *Revista Foreign Affairs en Español* 84, no. 6 (January-March 2006). Published by the Instituto Tecnológico Autónomo de México.

458 Hans Blix, *¿Desarmando a Irak?* (España: Planeta, 2004).

459 Melanie *Ramjoue, Improving United Nations Intelligence: Lessons from the Field*, GCSP Policy Paper no. 19 (August 2011), Geneva Centre for Security Policy, *http://www.gcsp.ch/content/download/6457/59721/download*.

460 On this point see Eduardo Aldunate, *Mision en Haiti* (Chile: Centro de Estudios Bicentenario, 2007). Also see Eduardo Aldunate, *Las razones politicas y morales de la mission ONU en Haiti* (Spain: FRIDE, 2008), *http://www.fride.org/download/COM_UN_Haiti_ESP_abr08.pdf* .

461 Julia Pulido, *op. cit.*; Antonio Diaz, Miguel Revenga, Oscar Jaime, and Rafael Martinez, "Hacia una política europea de inteligencia," *Revista Política Exterior* (Spain) XIX, no. 106 (August 2005).

462 Estatuto de Consejo de Defensa Suramericano, artículo 5, letra B, *Consejo de Defensa Suramericano: Crónica de su gestación* (Chile: Ministerio Defensa Nacional, 2009), p. 169. Document obtained from the Working Group of the South American Defense Council.

463 Jose Manuel Ugarte, "El Consejo de Defensa Suramericano: Naturaleza, balance provisorio, perspectivas y desafíos," in Hans Mathieu and Catalina Nino, eds., *Anuario 2010 de la Seguridad Regional en America Latina y el Caribe* (Colombia: Friedich Ebert Stiftung, 2010), p. 34.

464 Julia Pulido, *op. cit.*, p. 288.

465 Andres Gomez de la Torre, "Intereses académicos compartidos: hacia una comunidad iberoamericana de inteligencia," *Inteligencia y Seguridad: Revista de análisis y prospectiva* no. 2, Universidad Rey Juan Carlos, España (Cátedra Servicios de

Inteligencia y Sistemas democráticos) and Universidad Carlos III de Madrid (Instituto Juan Velásquez de Velasco de Investigación para la Seguridad y Defensa), 2007.

466 Andrea Carvalho and Miguel Esteban, "Los servicios de inteligencia: entorno y tendencias," in Jose Gonzalez, coord., *Inteligencia* (España: Tirant lo Blanch, 2012), p. 92.

467 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de Inteligencia," *Revista Política y Estrategia* (ANEPE) no. 120 (July-December 2012), p. 163.

468 For these points, the author has taken into account the works of Antonio Diaz, coord., Miguel Revenga, Oscar Jaime, and Rafael Martinez, "Hacia una política europea de inteligencia," *op. cit.*, and of Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia."

469 There are various ways of referring to the type of intelligence related to crime and to situations that may seriously affect public security. For example, one can refer to police intelligence, criminal intelligence, or police information. All these terms have the same referent, but with different breadths of meaning according to the organization involved. In the UNASUR region the police are responsible for police intelligence, but it is more usual in Spain to speak of police information services, and this is the term chosen for the present work because much of the referenced work is from Spain. Some authors in some countries distinguish police intelligence from criminal intelligence.

470 *Ibid.*, p. 62.

471 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de Inteligencia," p. 190.

472 MERCOSUR countries include Argentina, Brazil, Paraguay (presently suspended), Uruguay, Venezuela and Bolivia (in process of joining). Associate members include Chile, Colombia, Peru, Ecuador, Guyana (now in process of ratification), and Surinam (also in process of ratification). "Expanded" MERCOSUR refers to the set of full and associate members.

473 See Celina B. Realuyo, "Collaborating to Combat Illicit Networks through Interagency and International Effort," chapter 14 of Michael Miklaucic and Jaqueline Brewer, *Convergence: Illicit Networks and National Security in the Age of Globalization* (Washington, DC: National Defense University, 2013), *http://www.ndu.edu/press/convergence.html*. Accessed 13 April 2013.

474 Antonio Díaz Fernández, "Modelos de servicios de inteligencia en Europa y Latinoamérica," in Rafael Martinez and Joseph Tulchin, *El rompecabezas: Conformando la seguridad desde las dos orillas* (Spain: *Centre d'Informació i Documentació Internacionals a Barcelona*-CIDOB, 2006), p. 14.

475 Tim Schumacher, *Europas Geheimdienst: Das Joint Situation Centre*, 2011, *http://www.imi-online.de/2011/06/02/europas-geheimdienst/*. Accessed 15 February 2013.

476 Hans-Georg Wieck, *Multilaterale Zusammenarbeit der Geheimen Nachrichtendienste im Nordatlantischen Bündnis (NATO)–Ein Modell für die Europäische Union?*, p. 1, *http://www.hans-georgwieck.com/data/Eu%E4ische_Zusammenbarbeit_der_ND_Vortrag%20_042008.pdf*. Accessed 20 January 2013.

477 Julia Pulido, "El papel de la inteligencia en la PESD," *op. cit.*, p. 282.

478 Julia Pulido, "Inteligencia: la 'savia' de la Unión Europea," *Inteligencia y Seguridad: Revista de Análisis y Prospectiva*, no. 7 (December 2009-May 2010), pp. 92-93.

479 The organizational chart where one may schematically see where this organization fits appears at *http://eeas.europa.eu/background/docs/organisation_en.pdf*.

480 Chris Jones, "Secrecy Reigns at the EU's Intelligence Analysis Centre," *Statewatch*, no date, *http://www.statewatch.org/analyses/no-223-eu-intcen.pdf*. Also see Iikka Sami, *European Parliament*, no date, *http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede041011cvsalmi_/sede041011cvsalmi_en.pdf.*

481 Julia Pulido, "Inteligencia: la 'savia' de la Unión Europea," p. 87-107.

482 Tim Schumacher, *op. cit*.

483 Francisco Veiga, "*ECHELON, en control directo*," in *El desequilibrio como orden: Una historia de la posguerra fría 1990-2008* (Spain: Alianza Editorial, 2009).

484 Antonio Diaz Fernandez, *op. cit.*, p. 14.

485 Antonio Diaz, Miguel Revenga Oscar Jaime and Rafael Martinez, *op. cit.*, p. 31.

486 Antonio Diaz Fernandez, *op. cit.*, p. 32.

487 Antonio Diaz Fernandez, "Evolución de la cooperación europea en inteligencia," *Varia Historia* (Belo Horizonte, Brazil) 28, no. 47 (2012), pp.184-185.

488 Antonio Diaz, Miguel Revenga, Oscar Jaime and Rafael Martinez, *op. cit.*, p. 26.

489 Examples of cooperation may be found in Antonio Diaz, coord., Miguel Revenga, and Oscar Jaime, *Cooperación en Inteligencia* (Spain: Thomson Reuters / IUGM, 2009) and in Anselmo del Moral Torres, *Cooperación Policial en la Unión Europea* (Spain: Dirección General de la Policía, Ministerio del Interior/Dykinson, 2011).

490 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de Inteligencia," p. 194.

491 Foundational Treaty of UNASUR, *http://www.unasursg.org/index.php?option=com_content&view=article&id=290&Itemid=339*. Accessed 1 February 2013.

492 *Ibid*.

493 A more detailed examination of this idea may be found in Carolina Sancho, "Cooperación en inteligencia y UNASUR: Posibilidades y limitaciones," Anepe, Chile, 2013.

494 "Valores, principios y seguridad en la comunidad iberoamericana de naciones," *Cuaderno de Estrategia* no. 126, IEEE / Defense Ministry of Spain, *http://www.ieee.es/Galerias/fichero/cuadernos/CE-126.pdf*. Accessed 10 January 2013.

495 The author recommends a review of the web pages of each of these organizations, which she accessed 15 November 2012. The CLACIP web page is at *http://www.clacip.org/* and that for INTERPOL at *http://www.interpol.int/es/*.

496 National Research Council of the National Academies, *Maritime Security Partnerships* (Washington, DC: The National Academies Press, 2008), p. 217.

497 Extracted from the GAFISUD web page, *http://www.fatf-gafi.org/pages/financialactiontaskforceofsouthamericaagainstmoneylaunderinggafisud.html*. Accessed 15 November 2012.

498 Extracted from the GAFISUD web page.

499 Extracted from the Chilean Customs Office web page, *http://www.aduana.cl/prontus_aduana/site/artic/20070227/pags/20070227233346.html*. Accessed 1 March 2013.

500 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia," p. 175.

501 *Ibid*.

502 *Ibid*.

503 *Ibid.*, p. 183.

504 *Ibid*.

505 *Ibid.*, p. 194.

506 See the web page *http://www.unasursg.org/inicio/documentos/consejos-sectoriales/consejo-suramericano-en-materia-de-seguridad-ciudadana-justicia-y-coordinacion-de-acciones-contra-la-delincuencia-organizada-trasnacional*.

507 Richard A. Clarke and Robert K. Knake, *Guerra en la red* (Spain: Ariel, 2011).

508 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia," pp. 157-158.

509 *Ibid*, p. 160.

510 Monica Serrano, "Crimen transnacional organizado y seguridad internacional: cambio y continuidad," in Mats Berdal and Monica Serrano (compiladores), *Crimen transnacional organizado y seguridad internacional* (Mexico: Fondo de Cultura Económica, 2005), p. 47.

511 On this point, the author recommends Javier Jordan, "Introducción al análisis de inteligencia," Grupo de Estudios en Seguridad Internacional (GESI-Spain), 2011, *http://seguridadinternacional.es/gesi/es/contenido/introducci%C3%B3n-al-an%C3%A1lisis-de-inteligencia*, and Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), *https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/*. Both accessed 10 October 2012.

512 Monica Den Boer, "Cooperación para la aplicación de la ley y crimen transnacional organizado en Europa," in Mats Berdal and Monica Serrano (compiladores), *op. cit.*, p. 174.

513 It is also true that institutionalized intelligence cooperation as discussed in this essay likewise presents challenges. The U.S. experience is of interest in this respect. See Bridget Rose Nolan, "Information Sharing And Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center," Ph.D. dissertation, University of Pennsylvania, 2013.

514 An example has occurred recently in Bolivia, whereby a senior anti-drug official was detained as he engaged in illicit trafficking activity. His arrest has affected intelligence cooperation, especially with Chile, because the intelligence service he headed is now disrespected, not least because his detention occurred on Chilean soil in a joint operation with the U.S. Drug Enforcement Administration. For further information, see "Ex Zar antidrogas boliviano se declara culpable en EE.UU. de tráfico de drogas a través de Chile," *La Tercera*, 24 June 2011, *http://diario.latercera.com/2011/06/24/01/contenido/pais/31-73881-9-ex-zar-antidrogas-boliviano-se-declara-culpable-en-eeuu-de-trafico-a-traves-de.shtml*. Accessed 5 February 2013.

515 Jose Manuel Ugarte, "Aportes y propuestas para la cooperación de inteligencia," p. 161.

516 Judge Barrington Parker, referring to Richard Helms, former Director of the Central Intelligence Agency, who was accused of lying to a congressional commission during his tenure to protect the secrets of the CIA. Cited by Paul Gordon Lauren, "Ethics and Intelligence," in *Intelligence, Policy and Process*, Alfred C. Maurer, Marion D. Tunstall, and James M. Keagle, eds. (Boulder, Colorado: Westview Press, 1985), p. 72.

517 On the differences between national intelligence in a democratic state and a totalitarian state, see Jose Manuel Ugarte, "Sistemas de Inteligencia y Democracia," in Bernardo Arevalo de Leon, comp., *Función Militar y Control Democrático* (Guatemala City: UNOPS, El Amanuense, 2001), pp. 182-185.

518 Jose Manuel Ugarte, *ibid.*, pp. 177-236.

519 Adopted in San Jose, Costa Rica, 22 November 1969. See *http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm*. Accessed 23 January 2013.

520 Jose Manuel Ugarte, *El control público de la actividad de inteligencia en América Latina* (Buenos Aires: Editorial Ciccus, 2012), p. 88.

521 In Chile, the term "forces of order" is used to refer to police agencies, and in particular to the *Carabineros de Chile and the Policía de Investigaciones*.

522 The Colombian statute declares that "in every instance, interception of communications will be subject to procedures established by article 15 of the constitution and in accordance with the Criminal Procedures Code (Article 42, 3rd paragraph).

523 In this case, notwithstanding the existence of judicial control over democratic security established in legislation, namely article 6, number 4 and article 13 of Law 750, of 2010, *http://legislacion.asamblea.gob.ni/Normaweb.nsf/b92aaea87dac762406257265005d21f7/8c11614758755b3a062578240073f60a?OpenDocument*. Accessed 12 October 2012.

524 See Legislative Decree 18-2008, article 34.

525 Title V, On special procedures for obtaining information, articles 23 to 32.

526 Section 21, subsection 3 of the Canadian Security Intelligence Service Act.

527 See for example the Netherlands' Intelligence and Security Act of 2002, *https://www.aivd.nl/english/aivd/the-intelligence-and/#Documents*. Accessed 10 October 2012.

528 Law 9883, article 1, sections 2 and 4. See Jose Manuel Ugarte, "El ámbito normativo de la inteligencia interior en América Latina," *Revista Vária História* 28, no. 47 (Belo Horizonte), June 2012, *http://www.scielo.br*. Accessed 15 December 2012.

529 The council had one representative from the intelligence office of the Federal Police, one from the operations office of the Federal Highway Police, two from the Federal Treasury Office (specifically from the offices of finance and tax investigation), two from the Ministry of Defense, one representative from the president's Institutional Security Cabinet, one from the civil defense area of the Ministry of National Integration, and one from ABIN.

530 Although this slight was subsequently reduced by the creation of the National Council for the Chiefs of Police Intelligence (CONCOI), per Resolution 1/2009

of the SENASP-MJ, it remained evident that this step was only palliative in nature, given the weakness of the new organization.

531 The present author has described the rise of the phenomenon of criminal intelligence in Latin America in several articles, including: "La actividad de inteligencia en América Latina y el surgimiento de la inteligencia criminal," paper presented at the meeting of the Latin American Studies Association, 2007 (Montreal), *www.resdal.org* (accessed 10 October 2012); "La evolución de la actividad de inteligencia y de la inteligencia criminal en América Latina: Actualidad, dificultades, perspectivas y propuestas," paper presented at the meeting of the Latin American Studies Association, 2009 (Rio de Janeiro), and incorporated into Jose Manuel Ugarte, *Actividad de Inteligencia y Democracia en América Latina* (Saarbrücken, Germany: Editorial Académica Española, 2011).

532 I do not believe that the Chilean Strategic Center for the Analysis of Crime should be considered, strictly speaking, an organization dedicated to criminal intelligence. This is because of its limited role in carrying out the analysis of information sent to it by Chilean institutions that play a role in the penal system of the country. The actual analysis is conducted by individuals who represent those institutions. That is, the Strategic Center itself does not have the capability to carry out the functions of the intelligence cycle.

533 On the National Intelligence Model, see Jose Manuel Ugarte, "La inteligencia Criminal en el Reino Unido y Canadá," *2ª Parte, Revista de Policía y Criminalística*, no. 18 (March 2007), Editorial Policial, Buenos Aires.

534 A brief reference to the European intelligence model is found in Hugo Brady, *Europol and the European Criminal Intelligence Model: A Non-state Response to Organised Crime* (Spain: Real Instituto Elcano, 2007), *http://www.realinstitutoelcano.org/wps/portal/rielcano_eng/Print?WCM_GLOBAL_CONTEXT=/wps/wcm/connect/elcano/Elcano_in/Zonas_in/ARI126-2007*. Accessed 4 January 2013. The exchange of police information is addressed in the European Union and the Council of Europe programs of The Hague (2005/C 53/01) and of Stockholm (2010/C 115/01).

535 Decreed Law 2859 (of 1979), article 1, with text from Law 20426, *www.leychile.cl.* Accessed 25 December 2012. For historical reasons, this force is sometimes labeled the "Gendarmerie," but both this term and "Gendarmeria" are used in Chile.

536 Information available on the web page of the Chilean Gendarmerie, *www.gendarmeria.gob.cl*. Accessed 26 December 2012.

537 It began operations on 19 April 2011. Details about the Chilean Strategic Crime Analysis Center may be obtained at *http://www.seguridadpublica.gov.cl.* Accessed 4 January 2013.

538 The present author agrees with the idea (current principally in the UK and Australia) that crime analysis is part of criminal intelligence.

539 In Latin America, intelligence doctrine usually distinguishes an "organismo [agency] de inteligencia," or an "organismo técnico especializado en inteligencia," both of which have the capability to carry out all the functions of the intelligence cycle, from an "órgano de inteligencia," which is capable only of some of those functions. The organization of interest here, the Chilean Strategic Crime Analysis Center, is strictly an "órgano [organization] de inteligencia."

540 In the United States, Executive Order 12333 does not expressly mention the Federal Bureau of Prisons, which is part of the Department of Justice. Also in the United Kingdom, the Intelligence Services Act of 1994 does not mention prison intelligence, nor do the Italian intelligence law of 2007 or the Belgian Intelligence and Security Services Law of 1998. To the author's knowledge, no country's intelligence laws specifically refer to any agency that engages in prison intelligence.

541 See Jose Manuel Ugarte, "La actividad de inteligencia en América Latina: De las reformas formales a las reformas legales," paper presented at the meeting of the Latin American Studies Association, 2012 (San Francisco, California), *www.aaint-eligencia.cl*. Accessed 20 December 2012.

542 Elizabeth Sepper, "Democracy, Human rights, and Intelligence Sharing," *Texas International Law Journal*, 46 (Fall 2010), p. 150.

543 Article 1 of the Argentine Penal Code establishes that "this code will apply: 1) to crimes committed in, or whose effects are felt in, the territory of the Argentine nation, or in those places subject to its jurisdiction; 2) to crimes committed outside Argentina by agents or employees of Argentine authorities as part of their official duty." Similar measures exist in other countries.

544 For a discussion of the importance of a conceptual definition of intelligence, see Rodrigo Iennaco, *Inteligência Criminal e Denúncia Anônima* (Belo Horizonte: Arraes Editores, 2011).

545 Domício Proença, personal communication with the author.

546 *Ibid*.

547 Eduardo Estevez, "Estructuras y su aplicación en policías en proceso de reforma," in *Inteligencia policial–Compilación de textos* (Guatemala: Instituto de Enseñanza para el Desarrollo Sostenible, 2000), p. 38.

548 Corporateness or corporatism in this case should be understood in its negative sense, whereby colleagues in a given institution try hard to overlook their own mistakes as they compare themselves to those in similar institutions, acting in isolation in their own organization and giving priority to building up a pure and simple rivalry based on long-standing institutional differences—the opposite of engaging in cooperation.

549 Luiz Eduardo Soares, *Segurança tem saída* (Rio de Janeiro: Sextante, 2011; 1st edition - 2006), p. 33.

550 *Ibid.*, p. 117.

551 *Ibid.*, pp. 36, 63.

552 *Ibid.*, p. 118.

553 Decreto 3695, 21 December 2000. For more on this point see Priscila Brandão, *Serviços Secretos e Democracia no Cone Sul* (Niterói: Impetus, 2010).

554 In Brazil, "military police" are part of the armed forces, but only as a reserve force (article 144 of the Constitution), and are subordinated to the 26 states and the federal district. They are responsible for maintaining public order, whereas civil police conduct criminal investigations. See *http://www.pm.ro.gov.br/index.php/intra/pm.html* for coverage of each state's military police establishment.

555 Relatório Ministério da Justiça–I Seminário Nacional sobre Atividade de Inteligência de Segurança Pública, Blue Tree Park, Brasília-DF, 5-7 December 2001.

556 *Ibid*.

557 Decreto 4685, 29 April 2003.

558 Rômulo Gomes Fonini, *Compartilhamento de Informações entre os órgãos de inteligência de segurança pública no país*, monograph prepared for the Ministry of Higher Education Foundation/Newton Paiva (Belo Horizonte, 2010).

559 Several witnesses confirm being astounded by the decreased level of attention given to the students and the course itself, especially at the graduation ceremony.

560 Anonymous interview conducted in Brasília, 26 July 2006.

561 Portaria 22, published in *Diario Oficial*, 22 July 2009.

562 Resolução No. 1, Conselho Especial do Sistema de Inteligência da Segurança Pública, 15 July 2009.

563 National Public Security Doctrine, printed edition, declassified but with restricted distribution, shared with those who attended a meeting on the preparations for the 15th Pan-American Games, July 2007.

564 Robert Blitzer, "Attorney General Guideline Changes Impacting FBI Intelligence Collection Operations," George Washington University Homeland Security Policy Institute, 15 June 2011, *http://securitydebrief.com/2011/06/15/attorney-general-guideline-changes-impacting-fbi-intelligence-collection-operations/*. Accessed 27 December 2011.

565 For an analysis of the military budget, see Patricia de Oliveira Mattos, "Orçamento e Defesa Nacional: an analysis of the defense portion of the federal budget from 2000 to 2009," in III Seminário de Estudos: *Poder Aeroespacial e Estudos de Defesa* - Anais, 2010, v. II. pp. 439-459, *http://www.unifa.aer.mil.br/seminario3_pgrad/trabalhos/patricia-de-oliveira-matos.pdf*. Accessed 3 January 2012.

566 Decreto 7364, 23 November 2010, *http://www.jusbrasil.com.br/legislacao/1025747/decreto-7364-10*. Accessed 19 December 2011.

567 Leandro Fortes, "Nós, os inimigos," Seção Seu País, *Revista Carta Capital*, edição 668, 14 October 2011, *http://www.cartacapital.com.br/politica/nos-os-inimigos-2/*. Accessed 3 January 2012. Italics added by the author.

568 Domicio Proenca Junior and Eugenio Diniz, *Política de defesa no Brasil: uma análise crítica* (Rio de Janeiro: Edições Humanidades, 1998), p. 42.

569 For discussion of these points the author is grateful to Roberto Numeriano, author of *Serviços Secretos: a sobrevivência dos legados autoritários* (Recife: Editora Universitária, 2010), and Vladimir Brito, author of *Sistemas de inteligência no Brasil e nos Estados Unidos*, monografia de especialização (Fundação Escola Superior do Ministério Público de Minas Gerais, 2009) and *O papel informacional dos serviços secretos*, Master's thesis (Graduate Program in Information Sciences, Universidade Federal de Minas Gerais, 2011).

570 Monica Barroso Ferreira Lacerda, "Processo Cíclico e Análise de Inteligência Policial," essay received by the author on 1 June 2009 for publication in the forthcoming book *Inteligência de segurança pública: Teoria e prática no controle da criminalidade*.

571 Michael Bayer, *The Blue Planet: Informal International Police Networks and National Intelligence* (Washington, DC: National Defense Intelligence College, 2010), p. 19.

572 *Ibid*., p. 100.

573 *Ibid*., pp. 17, 18.

574 *Ibid*., pp. 13, 15.

575 *Ibid*., pp. 20, 21

576 *Ibid*., p. 18.

577 *Ibid*., pp. 57, 59.

578 Article 23, paragraph VIII of Law 12527 (2011).

579 Bayer, *The Blue Planet*, *op. cit*., p. 52.

580 *Ibid*.

581 *Ibid*., pp. 56, 59.

582 The federal police have their own doctrine, which is being updated even though the older version is still unavailable to many intelligence operators.

583 Relatório Ministério da Justiça–I Seminário Nacional sobre Atividade de Inteligência de Segurança Pública, Blue Tree Park, Brasília-DF, 5-7 December 2001.

584 See, for example, Edmund F. McGarrell, Joshua D. Freilich, and Steven Chermak, "Intelligence-led Policing as a Framework for Responding to Terrorism," *Journal of Contemporary Criminal Justice*, 23, no. 2 (May 2007): 142-58. Also Gregory F. Treverton et al., *Moving Toward the Future of Policing* (Washington, DC: RAND Corporation, 2011), pp. 32-39, *www.rand.org/content/dam/rand/pubs/.../2011/RAND_MG1102.pdf*. Accessed 9 January 2012.

585 For greater detail, see Lucia Dammert, coord., *Reporte del sector seguridad en América Latina y el Caribe* (Santiago: FLACSO Chile, 2007).

586 Organization for Economic Cooperation and Development, *Security System Reform and Governance* (Paris, OECD, 2005), p. 20, *http://www.oecd.org/dataoecd/8/39/31785288.pdf*. Accessed 1 July 2012.

587 Comision Interamericana de Derechos Humanos, *Informe sobre seguridad ciudadana y derechos humanos*, 2009, p. 31, *http://www.oas.org/es/cidh/docs/pdfs/SEGURIDAD%20CIUDADANA%202009%20ESP.pdf*. Accessed 1 July 2012.

588 Louis Garzarelli, "Correctional Administrators' Attitudes: Making a Difference in Correctional Intelligence Gathering and Sharing," *Corrections Today* (December 2004), p. 119.

589 Edgardo Amaya, *Populismo punitivo: el irracionalismo penal de hoy* [Security and Penal Justice blog], 19 September 2006, *http://seguridadyjusticia.blogspot.com/2006/09/populismo-punitivo-el-irracionalismo.html*. Accessed 1 July 2012.

590 Organization of American States, *Declaración sobre seguridad de las Américas* (2003), Section II (2) of the document, *www.oas.org/csh/ces/documentos/ce00339s02.doc*. Accessed 1 July 2012.

591 Claudia Fuentes and Francisco Rojas, *Promover la seguridad humana: marcos éticos, normativos y educacionales en América Latina y el Caribe* (United Nations Educational, Scientific and Cultural Organization, 2005), p. 52.

592 Garzarelli, *op. cit*., p.118.

593 Ben Crewe, "The Sociology of Imprisonment," in Yvonne Jewkes, ed., *Handbook on Prisons* (Portland, Oregon: Willan Publishing, 2007), pp. 123-51.

594 Brian Parry, "Intelligence: The key to Gang Suppression," *Corrections Today* (April 2006), p. 42.

595 Crewe, *op. cit.*, p. 125.

596 Dammert, *op. cit*., p. 123.

597 Ministerio de Seguridad, Presidencia de la Nacion, "Misión" (no. 8), *http://www.minseg.gob.ar/misión*. Accessed 1 July 2012.

598 "El gobierno crea la Secretaría de Inteligencia mediante un decreto," *Diario en línea Hoy* [Ecuador], 11 June 2009, *http://www.hoy.com.ec/noticias-ecuador/el-gobierno-crea-la-secretaria-de-inteligencia-mediante-un-decreto-352782.html.* Accessed 1 July 2012.

599 Jose Maria Villalta, Proyecto de ley Derogatoria de la Dirección de Inteligencia y Seguridad del Estado y reforma de la Ley General de Policía, Law 7410, 26 May 1994, with its modifications.

600 "Un proyecto crea inteligencia estratégica para asistir a Evo," *Radio FM Bolivia*, 15 January 2010, *http://www.fmbolivia.com.bo/noticia21536-un-proyecto-crea-inteligencia-estrategica-para-asistir-a-evo.html*. Accessed 1 July 2012.

601 "Mujica tiene en su escritorio texto del nuevo proyecto de inteligencia," *La Red 21* (Montevideo, Uruguay), 27 February 2011, *http://www.lr21.com.uy/politica/442693-mujica-tiene-en-su-escritorio-texto-del-nuevo-proyecto-de-inteligencia*. Accessed 1 July 2012.

602 "Crean comisión para redactar ley de inteligencia," *El País* (Montevideo, Uruguay), 23 November 2011, *http://www.elpais.com.uy/111123/ultmo-608285/ultimo-momento/crean-comision-para-redactar-ley-de-inteligencia/*. Accessed 1 July 2012.

603 Dammert, *op. cit*., p. 115.

604 Bruce D. Berkowitz and Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton, New Jersey: Princeton University Press, 1989).

605 For greater detail, see Lucia Dammert and Liza Zúñiga, *La cárcel: problemas y desafíos para las Américas* (Santiago, FLACSO Chile, 2008).

606 Parry, *op. cit*., pp. 42-45 and Garzarelli, op. cit., pp. 118-121.

607 Elizabeth Sepper, "Democracy, Human Rights and Intelligence Sharing," *Texas International Law Journal* 46, no. 1 (Fall 2010), pp. 151-207. For a larger-scale examination of this theme, see *International Intelligence Cooperation and Accountability*, Hans Born, Ian Leigh, and Aidan Wills, eds. (London and New York: Routledge, 2011).

608 Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information* (New York: Cambridge University Press, 2001), p. 137, and Michael Herman, "11 September: Legitimizing Intelligence?" *International Relations* 16, 2 (2002), p. 233.

609 Moises Naim, *Illicit: How Smugglers, Traffickers, and Copycats Are Hijacking the Global Economy* (New York: Doubleday, 2005). Like Sepper, Naim points out that the underworld of criminality frequents ungoverned international or supranational spaces and opts for informal collaboration across countries and cultures.

610 H. Bradford Westerfield, "America and the World of Intelligence Liaison," *Intelligence and National Security* 11, 3 (July 1996), pp. 523-524.

611 James Igoe Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2010), p. 4.

612 U.S. Code, title 50, chapter 15, subchapter III, section 413b, *http://www.gpo.gov/fdsys/pkg/USCODE-2009-title50/html/USCODE-2009-title50-chap15-subchapIII-sec413b.htm*. Accessed 3 January 2013.

613 With few exceptions such as the U.S. anti-corruption law—the Foreign Corrupt Practices Act of 1977 governing the actions of U.S.-based corporations in bidding for overseas contracts and ensuring transparency in financial accounting practices—and the supranationally sanctioned but rare rendition of notorious criminals to the International Criminal Court.

614 Westerfield, *op. cit*., p. 541.

615 Martin Rudner, "Hunters and Gatherers: The Intelligence Coalition against Islamic Terrorism," *International Journal of Intelligence and CounterIntelligence* 17 (2004), p. 215.

616 Alasdair Roberts, "Entangling Alliances: NATO's Security of Information Policy and the Entrenchment of State Secrecy," *Cornell International Law Journal* 36 (2003), pp. 353-354.

617 Sepper, *op. cit.*, footnote 99.

618 *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Official Government Edition (Washington, DC: U.S. Government Printing Office, 2004), pp. 256, 258, 266, 268, 275-276.

619 Examples of international conventions include the Geneva Protocols for protection of noncombatants and treatment of prisoners of war; various international human rights treaties; the Convention on International Trade in Endangered Species of Wild Flora and Fauna; and the United Nations' Convention on the Law of the Sea.

620 Robert O. Keohane, "The Concept of Accountability in World Politics and the Use of Force," *Michigan Journal of International Law* 24 (2003), 1124. The threshold for accountability requires two elements: 1) an effective mechanism for inquiring into the rationale for decisions, and 2) costly sanctions that can be imposed on transgressors.

621 *International Journal of Intelligence Ethics,* ISSN 2151-2868, a semiannual journal beginning Spring 2010.

622 For example, in the view of an outside observer of the National Security Agency, the UKUSA community constitutes "a unique supranational body, complete with its own laws, oaths and language, all hidden from public view." James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency—From the Cold War to the Dawn of a New Century* (New York: Doubleday, 2001), pp. 403-04.

623 Ryan Goodman and Derek Jinks, "How to Influence States: Socialization and International Human Rights Law," University of Chicago and Harvard Law School, Public Law & Legal Theory Research Paper Series, Paper no. 95, p. 41, find that acculturation by some states leading other states toward the adoption of positive human rights practices depends more on positive behavioral cues and thus "less on the properties of the rule than on the properties of the relationship of the actor to the community." *www.law.uchicago.edu/files/files/62-Jinks.pdf*. Accessed 25 July 2012.

624 Sepper, *op. cit.*, p. 164.

625 Peter Wright, *Spy Catcher: The Candid Autobiography of a Senior Intelligence Officer* (New York: Viking, 1987). From the inside dustcover flap: "…the British government has gone to great lengths to keep [this book] from being published…."

626 See Michael D. Bayer, *The Blue Planet, op. cit.*, p. 34 and chapter 2 generally. See *http://www.ndic.edu/press/18507.htm*.

627 On the rise of the public security concept, see Organization of American States at *http://www.oas.org/en/topics/public_security.asp*. For a review of several initiatives see International Peace Institute (formerly International Peace Academy), *Police Reform through Community-Based Policing: Philosophy and Guidelines for Implementation* (New York: 2004), *http://pksoi.army.mil/doctrine_concepts/documents/UN/POLICE_REFORM.pdf*. Jerry H. Ratcliffe, *Intelligence-Led Policing* (Portland, Oregon: Willan Publishing, 2008) addresses the growh of intelligence-led policing.

628 Sepper's distillation of Michael Herman, "Ethics and Intelligence after September 2001," *Intelligence and National Security* 19, 2 (Summer 2004), see especially 346-350.

629 Sepper, *op. cit.*, p. 202.

630 The most well-known evidence of this tendency is the secret rendition to partner states of selected "illegal extraordinary combatants." See Dana Priest, "CIA Holds Terror Suspects in Secret Prisons," *Washington Post*, 2 November 2005, *http://www.washingtonpost.com/wp-dyn/content/article/2005/11/01/AR2005110101644.html*. Accessed 3 January 2013.

631 Sepper, *op. cit.*, 203.

632 Sepper, *op. cit.*, 203-204.

633 Bayer, *The Blue Planet, op. cit.*, chapter 5.

634 Although comparative figures are difficult to certify because of the internal priorities of various agencies, the budget figures for national security intelligence compared to national law enforcement are illustrative of the imbalance. The Director of National Intelligence requested a budget of $55 billion for fiscal year 2012 for the National Intelligence Program, a figure that excludes the budget for military intelligence, according to reporting by Steven Aftergood in Secrecy News, 15 Feb 2011, *http://www.fas.org/blog/secrecy/2011/02/intelbud_request.html.* Meanwhile, only $8.3 billion was requested for all Federal Bureau of Investigation activities for fiscal year 2011. See *http://www.fbi.gov/news/testimony/the-fbi-budget-for-fiscal-year-2011.*

635 Mario Villarreal Diaz and Juan Jose Rico Urbiola, "La penalización de las actividades de inteligencia hostil en los órdenes subnacionales de gobierno en México: el caso 'Nuevo León,'" in Jose Julio Fernandez Rodriguez *et al., Cuestiones de Inteligencia en la Sociedad Contemporánea* (Madrid: Ministerio de Defensa, Instituto Español de Estudios Estratégicos, 2011), pp. 175-185, *http://www.portalcultura.mde.es/Galerias/publicaciones/fichero/Cuestiones_inteligencia.pdf*. Accessed 25 July 2012.

636 Jeanna Cullinan, "Veracruz, Mexico, Fires 980 Police in Corruption Purge," 20 October 2011, *http://insightcrime.org/insight-latest-news/item/1729-veracruz-mexico-fires-980-police-in-corruption-purge.* Accessed 3 January 2013.

637 Spencer Ackerman, "How the Pentagon's Top Killers Became (Unaccountable) Spies," *Wired Magazine*, 13 February 2012, *www.wired.com/dangerroom/2012/02/jsoc-ambinder/*. Accessed 2 September 2012.

638 A series of reports about military deployments to the state of Vera Cruz in Mexico in late 2011 was soon followed by a report of the vetting of police officials in the same state, as an example of the interaction of a national security institution with police agencies. Some relevant installments: "México: envían más tropas a

Veracruz para contener violencia," *Noticias 24*, 5 October 2011, *http://www.noticias24.com/actualidad/noticia/330158/mexico-envian-mas-tropas-a-veracruz-para-contener-violencia/*; Ronan Graham, "Mexico Installs Federal Forces in Operation to Secure Veracruz," 6 October 2011, *http://www.insightcrime.org/criminal-groups/mexico/gulf-cartel/item/1667-mexico-installs-federal-forces-in-operation-to-secure-veracruz*; "Veracruz suma 980 policias despedidos," *El Universal*, 10 october 2011, *http://www.eluniversal.com.mx/estados/82622.html*. Consulted 3 January 2013.

639 One of the authors interviewed members of the federal, local, and municipal police, as well as Mexican military personnel, whose tasks include (internal aspects of) national security.

640 Note that in comparison with the military, a police officer in Mexico does not receive support in obtaining a mortgage for housing, whereas the military have excellent benefits such as assistance in obtaining home mortgages, car loans, insurance of excellent quality, educational support and recreational facilities, among other things.

641 For more information, see Encuesta Nacional de Inseguridad (ENSI - 7), p. 106, *http://www.icesi.org.mx/estadisticas/estadisticas_encuestasNacionales_ensi7.asp*. Accessed 14 September 2012.

642 Human-source intelligence penetration of "el narco" occurs rarely enough to be newsworthy. See Ginger Thompson, "U.S. Agencies Infiltrating Drug Cartels across Mexico," *New York Times*, 24 October 2011, *http://www.nytimes.com/2011/10/25/world/americas/united-states-infiltrating-criminal-groups-across-mexico.html?pagewanted=1&_r=3*. Accessed 3 January 2013.

643 Public Law 99-433, "Goldwater-Nichols Department of Defense Reorganization Act of 1986."

644 Rogers does not use this phrase, but it perfectly captures the realm in which cyber crimes exist. The term was coined during the 1970s and is widely used in political science.

645 Essays in Section One point to legislative, judicial and executive branch oversight and supervision mechanisms in place almost everywhere across the region that will help overcome some of the obstacles related to the potential abuse of government power, such as inappropriate invasion of privacy. Citizens in every country can point to their own historical examples in which such violations occurred, and many have adopted provisions to protect against future abuses.

Swenson notes in his introductory essay the "emphasis given to individual, personal or citizen security" in the region. However, that balance is constantly thrown into question as policymakers debate appropriate responses to acts of terrorism. Only constant, vigilant oversight by watchdog organizations, formal oversight bodies and elected officials can build public trust in intelligence organizations and maintain it over time.

646 Rosalba Gamez Alatorre, "Información o formación, en el ciberespacio," *Contexto Educativo, Revista Digital de Educación y Nuevas Tecnologías* 4, no. 23 (2002).

647 Ana Rosa Velazco Lozada, "La educación continua como instrumento de desarrollo en el siglo XXI," *Tendencias, Revista de la Universidad Blas Pascal* 5, no. 10 (2011), p. 3.

648 Pablo Martinez, "Los nuevos desafíos de la inteligencia en la *Republica Argentina," Revista de la Escuela Nacional de Inteligencia* 1, no. 1, Segunda Época (2003), p. 21.

649 As an example, the Argentine National Intelligence School (ENI) has since 1999 offered a master's degree that is accredited within the official higher education system, with the support of the *Universidad Nacional de La Plata*. The program is open to anyone; only an undergraduate degree is required for all applicants. Over the course of its existence, the program has atttracted university professionals from different disciplines, lawyers, political scientists, engineers, and international relations specialists, among others.

650 Andres Gomez de la Torre Rotta, "Quien vigilará a nuestros vigilantes? (Reinventando a Juvenal ante el foro de Roma en Perú y Sudamérica)," *Inteligencia y seguridad: Revista de análisis y prospectiva* (Spain) no. 5 (December 2008-May 2009), pp. 49-50.

651 Paul Chaves, "Los Espías no Bastan: Definiendo las Políticas Públicas en Materia de Servicios de Inteligencia en Costa Rica," REDES 2001 (Research and Education in Defense and Security Studies), Center for Hemispheric Defense Studies, Washington, DC, 22-25 May 2001.

652 Miguel Angel Esteban Navarro *et al.*, "Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información," *El profesional de la información* 12, no. 5 (2003), p. 270.

653 Comments from the National Secretary of Intelligence, "Acto de clausura del VII curso especial de perfeccionamiento en inteligencia estratégica nacional SIGLO XXI," *Revista de la Escuela Nacional de Inteligencia* 7, no. 1 (Primer Trimestre 1998), p. 10.

654 Jesus Tramullas Sas, "Tecnologías para la gestión del conocimiento y la generación de inteligencia," I Seminario sobre Gestión del Conocimiento y Servicios de Inteligencia en el siglo XXl, Universidad Carlos III de Madrid, *Boletín Oficial del Estado*, Instituto Español de Estudios Estratégicos (Madrid, Ministry of Defense, April 2003), p. 67.

655 Tramullas Sas, *ibid*., p. 70.

656 Diego Navarro Bonilla, "Introducción," *Cuadernos de Estrategia* 127, Estudios sobre inteligencia: fundamentos para la seguridad internacional, Grupo de trabajo 5/03 (Instituto Español de Estudios Estratégicos, Ministry of Defense, Spain, 2003), p. 20.

657 Specialization: For this designation, the student must demonstrate mature handling and use of knowledge, to include writing, presenting, and gaining approval of a final product or thesis. Master's: This degree involves a variety of organized activities in a specific area of knowledge, including deep and systematic knowledge of a discipline and the application of suitable research methodology, to be demonstrated through the development of a thesis. Doctorate: Doctoral studies are oriented toward developing researchers who will make significant contributions to knowledge in a particular area, and developing those capabilities through carrying out original research in the form of a doctoral thesis.

658 Rocio Santamaria Ambriz, "Los desafíos del postgrado en América Latina," *Colección EDUAL* 6, (1995), p. 21.

659 Walter Barutia Feijoo, "Acreditación universitaria, retos y oportunidades," *Estudios en Ciencias Administrativas* 1, no. 1 (2003), of the *Universidad Nacional Mayor San Marcos, Facultad de Ciencias Administrativas, Unidad de Postgrado*, Peru, pp. 209-210.

660 Examples of the professionalization of intelligence personnel through higher education include Argentina (master's degree from the National Intelligence School/*Universidad de la Plata*); Chile (master's from the Chilean Army War College-*ACAGUE/Universidad de Chile*); and the United States (master's with the National Intelligence Unversity), although each of these countries has adopted different approaches.

661 Carlos Gustavo Arrieta P., *et al*., "Informe de la Comisión Especial para el DAS," Bogota, 2006. This article notes that "the Commission insistently recommends the establishment of periodic, external evaluation of the education provided by the intelligence school—a rigorous 'quality control system.' It should be started immediately, and subsequently, the outside review should be accomplished every five years. The commission also recommends permanent programs to meet the needs of intelligence professionals after they have passed through this school, so that they can update themselves on the best and latest techniques for obtaining, handling, and analyzing intelligence and counterintelligence."

662 See *http://www.esici.edu.co/*.

663 Relación de cursos impartidos por el CISEN (2000–2008). See *http://www.cisen.gob.mx/site/pdfs/doc_desclasificados/21_2008_CURSOS_CAPACITACION_2000-2008.pdf*. Accessed 16 May 2012.

664 Guillermo Valdez Castellanos, "Inteligencia para la Seguridad Nacional en el Siglo XXI," *CISEN: 20 anos de historia—Testimonios* (México: CISEN, Febrero 2009), pp. 14-15, *http://www.cisen.gob.mx/site/pdfs/actualidad/La_Inteligencia_seguridad_nacional_Valdes.pdf*. Accessed 16 May 2012.

665 See *http://www.cisen.gob.mx/site/cisen.htm*.

666 NIU makes its catalog of courses and research publications available at *http://www.ni-u.edu/index.html.*

667 Interview with the Director of CALEN, General Jose Burone, on 10 January 2012, published in *La Republica Digital, http://www.diariolarepublica.net/2012/01/calen-dictara-primer-curso-de-inteligencia-estrategica/.* Accessed 10 May 2012.

668 "By Decree 7662, the Bolivarian Military University of Venezuela (UMBV) is established," *Gaceta Oficial* of Venezuela, no. 39,502, 3 September 2010.

669 Russell G. Swenson, "¿Para qué sirve una escuela de inteligencia nacional?," Conferencia Magistral, Escuela Nacional de Inteligencia, Peru, 2007.

670 Alberto Bolivar Ocampo, "Prefacio," in Russell G. Swenson and Susana C. Lemozy, eds., *Intelligence Professionalism in the Americas* (Washington, DC: Joint Military Intelligence College, 2004), pp. 20-21, *http://www.ni-u.edu/ni_press/pdf/Intelligence_Professionalism_in_the_Americas.pdf*. Accessed 5 June 2012.

671 Jaime Castillo Arias, "Sistemas de Inteligencia: Perspectiva doctrinal para realizar un análisis integral," *Inteligencia estratégica y prospectiva* (Quito: Facultad Latinoamericano de Ciencias Sociales-FLACSO and Secretaría Nacional de Inteligencia del Ecuador, 2011), p. 98.

672 Alvaro Jose Venegas Gonzalez, "Comportamiento profesional en un Área de Análisis de Inteligencia Civil estatal colombiana," *Nova et Vetera* (Colombia) 19, no. 63 (2010), p. 131.

673 William Lynn III, co-originator of the "4th-generation warfare" concept, speaking at the Center for Strategic and International Studies (CSIS) Global Security Forum 2012, 11 April 2012, *http://csis.org/files/attachments/120411_FightingACyberWar_GSF_Transcript.pdf*. Accessed 11 August 2012.

674 U.S. President, *Cyberspace Policy Review*, 2009, p. 1, *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf*. Accessed 24 July 2012.

675 *Ibid*. This more complete definition comes from the U.S. executive branch document, National Security Presidential Directive 54/Homeland Security Presidential Directive 23. Most of this document is classified; therefore, only the cyberspace policy review is cited.

676 IT Business Edge, "Cyberspace" definition, *http://www.webopedia.com/TERM/C/cyberspace.html*. Accessed 24 July 2012.

677 Cyberspace.cz, "Cyberspace" definition, *http://www.cyberspace.cz/*. Accessed 24 July 2012.

678 Dan Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security* (Washington, DC: National Defense University Press, 2009), *www.carlisle.army.mil/dime/getDoc.cfm?fileID=181, p. 4*. Accessed 24 July 2012.

679 Although a full discussion of the legal implications of stopping just short of including information itself falls beyond the scope of this essay, one entanglement from doing so would appear in those countries that apply fraud laws to an intruder who gains unauthorized access in cyberspace (see the discussion on "intrusion" in the present essay), and then also apply theft laws for the information that was accessed.

680 "Cyberattack" definition in Technopedia, *http://www.techopedia.com/definition/24748/cyberattack*. Accessed 24 July 2012.

681 This definition comes in part from U.S. Joint Chiefs of Staff, *JP 1-02 U.S. Department of Defense Dictionary of Military Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf*. Accessed 24 July 2012.

682 This definition comes from information posted on the U.S. Federal Bureau of Investigation website *http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions*. Accessed 25 July 2012.

683 Paraphrased from U.S. Government Printing Office, Title 18, U.S. Code § 1030, "Fraud and Related Activity in Connection with Computers," *http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap47-sec1030.pdf*. Accessed 25 July 2012.

684 U.S. Department of Commerce, National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Washington, DC: October 1995), *http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/index.html*. Accessed 30 August 2012.

685 "Private" in this use indicates limited access. Thus, a government computer or network that requires an individual password or other specific authorization is considered private, just like a private-sector computer or network.

686 David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution*, IDA Paper P-3792 (Washington, DC: Institute for Defense Analyses, October 2003), p. 1.

687 Those curious about LOIC can simply search for "LOIC" on Google.

688 For more detail about botnets and the effects that they can cause, see "Bots & Botnet: An Overview," *http://www.sans.org/reading_room/whitepapers/malicious/bots-botnet-overview_1299*. Accessed 25 July 2012.

689 U.S.-CERT, "Cyber Threat Source Descriptions," *http://www.us-cert.gov/control_systems/csthreats.html#nat*. Accessed 25 July 2012.

690 John Brodkin, "Government-sponsored cyber attacks on the rise, McAfee says," Networkworld.com, 29 November 2007, *http://www.networkworld.com/news/2007/112907-government-cyberattacks.html*. Accessed 25 July 2012.

691 Anna Mulrine, "China is a lead cyberattacker of US military computers, Pentagon reports," *Christian Science Monitor*, 18 May 2012, *http://www.csmonitor.com/USA/Military/2012/0518/China-is-a-lead-cyberattacker-of-US-military-computers-Pentagon-reports*. Accessed 26 July 2012.

692 Joel Brenner, *America the Vulnerable* (New York: Penguin Press, 2011), pp. 27-28. All of Chapter 2 (pp. 25-43) presents a useful overview of cyber criminal activity.

693 Price WaterhouseCoopers Brazil, Ltda, *Cybercrime: Protecting against the Growing Threat—Global Economic Crime Survey*, November 2011, *http://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf.* Accessed 26 July 2012.

694 Norton.com, "Cybercrime Report for 2011," *http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf*. Accessed 4 September, 2012.

695 Phil Muncaster, "Patriotic hackers face off in South China Sea: Dispute over islands claimed by China and Philippines goes online," 27 April 2012, *http://www.theregister.co.uk/2012/04/27/philippine_china_hack_stand_off/*. Accessed 11 August 2012.

696 Kim Zetter, "Report: Hacktivists Out-Stole Cybercriminals in 2011," *Wired Magazine*, Threat Level blog, 22 March 2012, *http://www.wired.com/threatlevel/2012/03/hacktivists-beat-cybercriminals/*. Accessed 11 August 2012.

697 "Kaspersky Security Bulletin: Malware Evolution 2011," *Securelist*, 1 March 2012, *http://www.securelist.com/en/analysis/204792217/Kaspersky_Security_Bulletin_Malware_Evolution_2011*. Accessed 14 August 2012.

698 Parmy Olson, *We Are Anonymous* (New York: Little, Brown and Company, 2012), pp. 93-94 and 107-12.

699 Press Association, "Anonymous claims responsibility for taking down government sites," *The Guardian*, 8 April 2012, *http://www.guardian.co.uk/technology/2012/apr/08/anonymous-taking-down-government-websites*. Accessed 11 August 2012.

700 Olson, *op. cit.*, pp. 280-282.

701 Brian Emery, "LulzSec hits Brazilian websites," *BBC News*, 22 June 2011, *http://www.bbc.co.uk/news/technology-13878888*. Accessed 11 August 2012.

702 THN Security Analyst, "Lulzsec hack Infraguard Atlanta Members Alliance & challenge FBI!" *Hacker News*, 3 June 2011, *http://thehackernews.com/2011/06/lulzsec-hack-infragard-atlanta-members.html*. Accessed 11 Aug 2012.

703 Ellen Nakashima, "CIA Web Site Hacked; Group LulzSec Takes Credit," *Washington Post*, 15 June 2011, *http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html*. Accessed 11 August 2012.

704 John Markoff, "A Most-Wanted Cyberthief Is Caught in His Own Web," *New York Times*, 16 February 1995, *http://www.nytimes.com/1995/02/16/us/a-most-wanted-cyberthief-is-caught-in-his-own-web.html*. Accessed 12 August 2012.

705 Kevin Mitnik, *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* (New York: Little Brown and Company, 2011), p. 385.

706 U.S. Government Printing Office, 42 USC § 5195c-"Critical Infrastructures Protection," *http://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf*. Accessed 16 August 2012.

707 For a graphic representation of the comparative proportion of Internet users in Brazil and the United States over time, see Google.com at *http://www.google.com/publicdata/explore?ds=d5bncppjof8f9_&met_y=it_net_user_p2&idim=country:BRA&dl=en&hl=en&q=brazil+internet+usage#!ctype=l&strail=false&bcs=d&nselm=h&met_y=it_net_user_p2&scale_y=lin&ind_y=false&rdim=region&idim=region:NAC&idim=country:BRA:USA&ifdim=region&hl=en_US&dl=en&ind=false*. Accessed 16 August 2012.

708 "For the Satellite Industry, Lines Blur Between Military and Commercial Markets," *National Defense Magazine* blog, 18 March 2011, *http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=350*. Accessed 16 August 2012.

709 The U.S. Federal Information Security Management Act of 2002 assigns responsibilities and authorities for providing cybersecurity to federal agencies and other executive branch organizations. For further information on this law, see: U.S. Government Printing Office, 44 USC § 3541-"Federal Information Security Management Act of 2002," *http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3541.pdf*. Accessed 6 September 2012.

710 All information about the seven centers comes from the illustration "National Cybersecurity Center Policy Capture," posted on the White House website at *http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf.* Accessed 16 August 2012.

711 See the Brazilian home page at *http://www.cert.br/en/* for further details about the CERT.br mission and subordination. Accessed 17 August 2012.

712 For a brief summary of SERPRO, see *http://www.securities.com/Public/company-profile/BR/SERPRO_en_1154549.html*. Accessed 17 August 2012. The serpro portal (serpro.gov.br) is in Portuguese.

713 Luiz Fabricio Thaumaturgo Vergueiro, "Brazilian Security Structure," Federation of American Scientists Intelligence Research Program, *http://www.fas.org/irp/world/brazil/fabrverg.pdf*. Accessed 17 August 2012.

714 European Union, *EU/COE Joint Project on Regional Cooperation against Cybercrime: Specialised cybercrime units—Good Practice Study*, Version 9, November 2011, *http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/2467_HTCU_study_V30_9Nov11.pdf.* Accessed 17 August 2012.

715 Isabel Estrada, "Cyberspace Becomes Newest Battlefield for Brazil's Armed Forces," *Diálogo-Américas*, 8 March 2011, *http://dialogo-americas.com/en_GB/articles/rmisa/features/regional_news/2011/08/03/aa-brazil-cyber-warfare*. Accessed 17 August 2012.

716 Marco Cepik and Priscila Antunes, "The New Brazilian Intelligence Law: An Institutional Assessment," paper presented at Center for Hemispheric Defense Studies, Research and Education in Defense and Security Studies, 22-25 May 2001, Washington, DC, *http://www.fas.org/irp/world/brazil/index.html*. Accessed 5 September 2012.

717 *Linha Defensiva*, 12 May 2012, *http://www.linhadefensiva.com/2012/05/brazilian-army-prepares-its-cdciber-the-cyber-defense-center/*. Accessed 17 August 2012.

718 Nelson de Sa, "General detalha implantação do Centro de Defesa Cibernética, novo órgão brasileiro," Folha de São Paolo, 5 July 2012, in Portuguese at *http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml*. Accessed 5 September 2012.

719 Emerson Wendt, "Ciberguerra, inteligência cibernética e segurança virtual: alguns aspectos," in GSI publication *Revista Brasileira de Inteligência*, no. 6 (April 2011), p. 22, *http://www.abin.gov.br/modules/mastop_publish/files/files_4e3ae31e2c097.pdf*. Accessed 5 September 2012.

720 For further information, see *http://www.cert.br/en/*. Accessed 12 September 2012.

721 Whichever of the communities may be responsible for the national CERT should have a great deal of information about the intrusion. The responsible group may not be able to provide immediate attribution (who), but it will be able to discern some of the details about where the intrusion came from—or passed through. Country A may have several overlapping CERTs, each of which would have some knowledge of the intrusion. If that were the case, then the importance of sharing information is even greater: any one of the CERTs may have important information that the others do not. Overlap of CERT responsibilities is important to intelligence managers because it may increase the number of organizations with which intelligence information about the intrusion needs to be exchanged.

722 The U.S. Intelligence Community's obligation to protect information extends to protecting personal information that may be gathered coincidentally in efforts to gather foreign intelligence. U.S. law strictly limits with whom such information may be shared, and even how it may be stored, if it may be stored at all. For further reading, see U.S. Government Printing Office, 50 USC § 36, *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, http://www.gpo.gov/fdsys/pkg/PLAW-110publ261/html/PLAW-110publ261.htm*. Accessed 5 September 2012. In the United States, individual states can perhaps address cyber security in the more comprehensive and aggressive fashion envisioned by Michael J. Glennon in "State-Level Cybersecurity," *Policy Review* (February-March 2012).

723 United States Office of the Director of National Intelligence, Intelligence Community Directive Number 208 "Write for Maximum Utility," 17 December 2008, *http://dni.gov/files/documents/ICD/icd_208.pdf*. Accessed 24 August 2012.

724 *Ibid*.

725 U.S. Government, Executive Order 12333, paragraph 1.7, "U.S. Government Intelligence Activities," 4 December 1981, *http://www.gpo.gov/fdsys/pkg/FR-2008-08-04/pdf/E8-17940.pdf*. Accessed 28 August 2012.

726 Organization of American States, "A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating

a Culture of Cybersecurity," 2004, *http://www.oas.org/juridico/english/cyb_pry_strategy.pdf*. Accessed 29 August 2012.

727 Gen. Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly* (Spring 2011), p. 4, *http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf*. Accessed 5 September 2012.

728 *Ibid*.

729 Senator Dianne Feinstein, "Feinstein Calls on Obama to Protect Computer Networks from Cyber Attacks," 28 August 2012, *http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=8c64f8e4-6780-4a4f-88eb-cd26a8839aae*. Accessed 6 September 2012.

730 "GCHQ to advise senior business leaders on how to fight cyber attacks," *The Telegraph* at telegraph.co.uk, 6 September 2012, *http://www.telegraph.co.uk/news/uknews/defence/9521715/PLS-PIC-AND-PUB-GCHQ-to-advise-senior-business-leaders-on-how-to-fight-cyber-attacks.html*. Accessed 6 September 2012.

731 Eric Ensign, *Intelligence in the Rum War at Sea, 1920-1933* (Washington, DC: Joint Military Intelligence College, 2001), *http://www.ni-u.edu/ni_press/pdf/Intelligence_Rum_War.pdf.*

732 *ISAF Security Force Assistance Guide*, April 2013. *https://ronna-afghan.harmonieweb.org/CAAT/Shared%20Documents/20130505_NIU_SFA_Guide.pdf. Accessed 5 August 2013. Also see Liz Panarelli, The Role of the Ministerial Advisor in Security Sector Reform (Washington, DC: U.S. Institute for Peace, April 2009), http://www.usip.org/files/resources/USIP_0409.PDF*. Accessed 7 May 2013.

733 It is also underpinned by an internationally binding legal regime to which foreign forces are subject upon sovereign recognition. See Major Andrew R. Atkins' discussion of the complexities of host-nation sovereignty recognition in military operations in his "Doctrinally Accounting for Host Nation Sovereignty during U.S. Counterinsurgency Security Operations," *Military Law Review* 212 (Summer 2012), pp. 70-132.

734 Sarah Meharg and Aleisha Arnush, although they do not directly reference smart power, make a similar argument when they note that "[a]ccording to the U.S. Army's *Field Manual* (FM) 3-07, *Stability Operations* (2008) [also emphasized in its successor Field Manual (FM) 3-22, see fn. 777 below], SSR is an activity that can reinforce diplomatic and defense interventions while reducing long-term se-

curity threats by building capacities for stable, prosperous, and peaceful societies." See their *Security Sector Reform: A Case Study Approach to Transition and Capacity Building* (Carlisle, Pennsylvania: Peacekeeping Stability Operations Institute Paper, Security Studies Institute, U.S. Army War College, December 2010, p. 7, *http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=960*. Accessed 17 October 2012

735 See *United States Department of the Army, Field Manual (FM) 3-22: Army Support to Security Cooperation* (January 2013), paragraphs 4-57 and 4-58: "The advise task for the governmental level [SSR] is aimed at advising a foreign government's high-ranking personnel at their national, federal, departmental, or ministerial level. U.S. agencies outside the DOD provide nonmilitary advice. The advise task at the governmental level must involve a whole-of-government effort integrating U.S. agencies such as the Departments of State, Treasury, and Justice.… DOD initiated the Ministry of Defense Advisors (known as MoDA) program to forge long-term relationships that strengthen a partner nation's defense ministry."

736 Richard L. Armitage and Joseph S. Nye, Jr., *CSIS Commission on Smart Power* (Washington, DC: Center for Strategic and International Studies, 2007), p. 7, *http://csis.org/files/media/csis/pubs/071106_csissmartpowerreport.pdf*. Accessed 13 July 2012. In this chapter the authors take an agnostic view toward smart power and limit discussion to its operational impacts on security sector reform and intelligence management.

737 See Joseph A. Nye for a full explanation of his concept of soft power in national security and foreign affairs in *Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), and *Bound to Lead: The Changing Nature of American Power* (New York: Basic Books, 1990).

738 In John J. Hamre's interview with key smart power thinkers Richard L. Armitage and Joseph Nye, they agreed that the smart power approach necessarily involves "ced[ing] some national sovereignty," particularly "when working within international institutions" (Hamre) but that "every successful relationship requires compromise" (Armitage) and "the benefits outweigh the costs to us" (Nye). See "Smart Power: John J. Hamre talks with Joseph Nye & Richard Armitage" *The American Interest* 3, no. 2 (November/December 2007), pp. 34-41.

739 Sarah Meharg and Aleisha Arnush, *op cit.*, p. iii.

740 David Axe, "The Limits of Smart Power," *The American Prospect* 21, no. 10 (December 2010), pp. 23-27; Nicholas J. Armstrong, "Afghanistan 2014-2024:

Advising for Sustainability," *Small Wars Journal* (4 May 2012), *http://smallwarsjournal.com/author/nicholas-j-armstrong*. Accessed 4 October 2012.

741 *United States Department of the Army Field Manual 3-22*, paragraph 1-61.

742 Liz Panarelli, *op. cit*, p. 2.

743 *Ibid*., p. 2.

744 Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011).

745 Suzanne Nossel, "Smart Power: Reclaiming Liberal Internationalism," *Foreign Affairs 83*, no. 2 (March/April 2004), pp. 131-142.

746 Johanna Mendelson Forman, "Investing in a New Multilateralism–A Smart Power Approach to the United Nations," Center of Strategic and International Studies, Smart Power Initiative (January 2009), *http://csis.org/files/media/csis/pubs/090128_mendelsonforman_un_smartpower_web.pdf, 1-14*. Accessed 5 August 2013.

747 Stephen M. Saideman and David P. Auerswald, "Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan," *International Studies Quarterly* 56 (March 2012), pp. 67-84.

748 William B. Caldwell and Nathan K. Finney, "Building Police Capacity in Afghanistan: The Challenges of a Multilateral Approach," *Prism 2*, no. 1 (December 2010), pp. 121-129, *http://www.ndu.edu/press/lib/images/prism2-1/Prism_121-130_Caldwell-Finney.pdf*. Accessed 16 October 2012.

749 Dennis Steele, "The Closers," *Army Magazine* 60, no. 4 (April 2010), pp. 58-66. The 3rd Infantry Division was tasked with providing support to the Department of State's Provincial Reconstruction Teams while carrying out its advise and assist mission to Iraqi security forces development. Nicole Ball provides a comprehensive explanation of the functional intersections in security sector reform in "Enhancing Security Sector Governance: A Conceptual Framework for UNDP," Consultant Report (October 2002), Table 1, p. 14, *http://www.ssrnetwork.net/uploaded_files/3202.pdf*. Accessed 5 September 2012.

750 LTG William B. Caldwell IV, with Derek S. Reveron, "Surging Security Force Assistance in Afghanistan," *Military Review* (November-December 2011), p. 19.

751 Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Doubleday, 1959). See Mark R. Leary and Ashley Batts Watson, "Personality and Persona: Personality Processes in Self-Presentation," *Journal of Personality* 79, no. 6 (December 2011), pp. 889-916 for an excellent extension of Goffman's seminal concepts.

752 For more on the Ministry of Defense Advisors Program see *http://www.defense.gov/home/features/2011/0211_moda/*. For the Afghanistan-Pakistan Hands Program see *http://www.jcs.mil/page.aspx?id=52*.

753 David A. Klein, "The Strategic Management of Intellectual Capital: An Introduction" in David A. Klein, ed., *The Strategic Management of Intellectual Capital* (Woburn, Massachusetts: Butterworth-Heinemann, 1998), pp. 2-3.

754 Mike Pedler, John Burgoyne, and Tom Boydell, *The Learning Company: A Strategy for Sustainable Development*, second edition (London: McGraw-Hill, 1997).

755 David A. Klein, *op. cit.*, p. 3.

756 *Ibid.*, p. 4.

757 *Ibid.*, p. 4.

758 Mary M. Crossman, Henry W. Lane and Roderick E. White, "An Organizational Learning Framework: From Intuition to Institution," *Academy of Management Review* 24, no. 3 (1999), p. 522, citing James G. March, "Exploration and Exploitation in Organizational Learning," *Organization Science*, 2 (1991), pp. 71-87.

759 United Kingdom Ministry of Defence, *Understanding and Intelligence Support to Joint Operations*, third edition, Joint Doctrine Publication 2-00, 30 August 2011.

760 *Ibid.*, p. 1-7.

761 *Ibid.*, p. 1-8.

762 *Ibid.*

763 *Ibid.*

764 *Ibid.*

765 *Ibid.*

766 *Ibid*.

767 In some instances the advising relationship is very close and the advisor is regarded as a confidant. When this happens the counterpart may provide insightful understanding by revealing a full explanation of the problem. Though it is extraordinarily valuable for an advisor and the advising mission's leadership to have such direct insight, that insight nonetheless still needs to be corroborated because the counterpart may, without prejudice, be misinformed or misunderstand the problem.

768 Director for operational plans and joint force development (J-7), *Joint Operations*, Joint Publication 3-0 (3 August 2011), III-11.

769 For a broader, historical perspective on variations in commitment levels among alliance members, see Patricia A. Weitsman, *Dangerous Alliances: Proponents of Peace, Weapons of War* (Stanford, California: Stanford University Press, 2004), especially p. 35.

770 Thomas Scott Gibson (TRADOC), "CALL publishes Company Intelligence Support Team Handbook," Center for Army Lessons Learned, Fort Leavenworth (25 January 2009), *http://www.army.mil/article/33509/call-publishes-company-intelligence-support-team-handbook/*. Accessed 5 August 2013.

771 Joint Chiefs of Staff, AFPAK Hands (APH) Program Overview Brief (26 August 2011), *http://www.jcs.mil//content/files/2011-09/090811135844_AFPAK_Hands_Program_Brief.pdf* Accessed 27 October 2012.

772 *http://www.defense.gov/home/features/2011/0211_moda/*. Accessed 6 July 2013.

773 David A. Klein, "The Strategic Management of Intellectual Capital: An Introduction," *op. cit*., p. 3.

774 Tony Bush, in *Theories of Educational Leadership and Management* (United Kingdom: Sage Publications, Ltd., 2010), draws from the organizational dynamics literature to summarize seven distinctions between organizational authority and influence.

775 See Michael T. Flynn, James Sisco, and David C. Ellis, "Left of Bang: The Value of Sociocultural Analysis in Today's Environment," *Prism 3*, no. 4, pp. 13-21, *http://www.ndu.edu/press/lib/pdf/prism3-4/prism12-21_flynn-sisco-ellis.pdf*. Accessed 2 June 2013. Note the National Geospatial Intelligence Agency's emphasis on human geography equally with physical features and imagery intelligence (National

Geospatial Intelligence Agency, "NGA Strategy 2013-2017," *https://www1.nga.mil/About/NGAStrategy/Documents/19639_NGA%20Strat%20Pub_Public_Web.pdf*, accessed 3 June 2013, as well as the Office of the Undersecretary for Defense Intelligence 2010 formalization of Activity-Based Intelligence (ABI) and Human Domain Analytics (HDA).

Index