NATIONAL INTELLIGENCE UNIVERSITY

Ann Caracristi Institute For Intelligence Research

RESEARCH FELLOWSHIP

RESEARCH MONOGRAPH

The Warning Renaissance

Advancing the Art and Science of Warning in the US Intelligence Community and Beyond

Johnathan Proctor, Joint Chiefs of Staff Directorate for Intelligence (JS J2)

Research Fellow, National Intelligence University, 2021–2023

The Warning Renaissance

Advancing the Art and Science of Warning in the US Intelligence Community and Beyond

Johnathan Proctor, Joint Chiefs of Staff Directorate for Intelligence (JS J2)

RESEARCH FELLOW, NATIONAL INTELLIGENCE UNIVERSITY, 2021–2023

PUBLISHED SPRING 2024

The views expressed in this *Research Monograph* are those of the author and do not reflect the official policy or position of National Intelligence University, Office of the Director of National Intelligence, or any other US Government agency.

Abstract

While warning has been written about for decades, surprisingly little consensus exists within the Intelligence Community (IC) about how to define and describe it. The use of terms such as strategic, operational, tactical, political, threat, and incident warning occurs across the scholarly and practitioner literature, often contradicting one another. Furthermore, within the field of intelligence studies, warning lacks an underlying theory of practice. This National Intelligence University (NIU) *Research Monograph* addresses the gap in this field by applying a data-driven research methodology to understand warning and then establish a foundational theory of warning through a two-step process. First, it employs grounded theory to explore the existing literature and practitioner perspectives on warning to identify seven foundational principles of warning. Second, it incorporates these principles to create an underlying theory of warning through the creation of a core lexicon, formal models of key concepts, and a framework of warning. As a central lexicon, three core definitions of warning emerge from the data: warning as a mission, warning as communication, and warning mindset. Meanwhile, the resulting framework establishes four functions of warning: exploratory warning, transition warning, dynamic warning, and explicit warning. Finally, this *Monograph* highlights those topics and issues requiring additional research and exploration, as well as implications from the proposed theory of warning on contemporary debates.

This page is intentionally left blank.

Key Findings and Recommendations

Warning guards a nation against surprise, ensuring decisionmakers accurately understand the full landscape of threats and opportunities they face. In pursuit of warning, intelligence services explicitly communicate those threats and opportunities to achieve an effect, prompting and enabling an informed response to address, prevent, or mitigate a threat. This warning-response process occurs within the context of both the threat landscape and the broader operational environment.

Data analysis of the warning literature and practitioner impressions identify seven foundational principles of warning.

1. Warning counteracts and mitigates surprise.
2. Warning requires a distinct mindset, focused on possibilities over probabilities and cognizant of the impacts of uncertainty, ambiguity, and complexity on how we view the world.
3. Warning must be timely and account for time, ensuring decisionmakers have the requisite temporal space needed to make and enact decisions.
4. The complete nature of the warning mission occurs across a broad spectrum of identifying, triaging, and tracking threats.
5. Warning is an explicit communication.
6. Warning seeks to persuade decisionmakers and prompt distinct decision points.
7. Warning occurs within a critically important relationship between intelligence and policy.

Existing definitions of warning that focus on comparing strategic and tactical warning have formed the dominant paradigm of warning throughout the subject's history, but this paradigm is insufficient in practice, potentially creating misunderstanding and inefficiency. These terms should be phased out of common use and replaced with a core warning lexicon that defines warning in the following three ways:

1. Warning as a mission.
2. Warning as a communication.
3. Warning as a mindset.

Within the full scope of the warning mission, there are four functions of warning which must be managed.

1. Exploratory warning, which seeks to understand the ever-changing threat landscape to inform decisions on strategy, planning, and resource allocation.
2. Transition warning, which closely monitors specific threats to inform decisions implementing associated plans, taking preventive action, or mitigating possible costs.
3. Dynamic warning, which informs more tactical decisions to posture forces and resources for advantage within a dynamic crisis environment.
4. Explicit warning, which ensures warnings are purposely and persuasively communicated to those decisionmakers with the authority and responsibility to act.

To completely accomplish the warning mission, an intelligence agency, enterprise, or community must execute all four warning functions while maintaining an active warning mindset. This mindset stands in stark contrast to the more traditional intelligence analysis mindset of most likely assessments established and maintained as an analytic line.

Contents

List of Figures

List of Tables

This page is intentionally left blank.

Glossary of Abbreviations and Key Terms

Cassandra Coefficient: A framework developed by Richard A. Clarke and R. P. Eddy to help decision-makers differentiate a legitimate warning from the field of extraneous "chicken little" warnings.[1]

CIA: Central Intelligence Agency

DCI: Director of Central Intelligence. The director of the Central Intelligence Agency who, before the establishment of the Director of National Intelligence, acted as the head of the US Intelligence Community.

DCID: Director of Central Intelligence Directive. The precursor of Intelligence Community Directives. Policy documents governing the performance and execution of the Intelligence Community before the Director of National Intelligence was established.

DIA: Defense Intelligence Agency

DoD: Department of Defense

DWN: Defense Warning Network. The DoD's formal warning apparatus as established in DoD Directive 3115.16.[2]

EAAWA: Every Analyst A Warning Analyst. The idea that all intelligence analysts across a nation's intelligence community inherently function as warning analysts. Used specifically by John Gentry and Joseph Gordon[3] as a "type of warning institution" in a nation that does not have a cadre dedicated to the warning function.

Grounded Theory: A systematic, yet flexible research methodology for collecting and analyzing qualitative data to construct theories from that data; thus, the research process constructs a theory "grounded" in the data.[4]

IC: Intelligence Community. A federation of 18 executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

JP: Joint Publication. An entry in the series of doctrine documents that present the fundamental principles guiding the employment of US military forces in coordinated and integrated action toward a common objective.

JSTOR: Stands for Journal Storage; a digital library that provides libraries and scholars with access to vast holdings of journal articles, books, images, and primary sources across 75 disciplines for research and study purposes.

NIO/W: National Intelligence Officer for Warning. Former position within the National Intelligence Council (NIC) that focused explicitly and exclusively on providing warning to national decisionmakers.

NATO: North Atlantic Treaty Organization

NIS: National Intelligence Strategy. Office of the Director of National Intelligence-produced strategic guidance document which provides the IC with strategic direction for a four-year period.

NIU: National Intelligence University. The IC's accredited, Federal degree-granting institution attended by intelligence and national security professionals.

NSC: National Security Council

ODNI: Office of the Director of National Intelligence. The head of the US Intelligence Community.

OODA Loop: Observe, Orient, Decide, Act Loop. A decisionmaking model developed by former Air Force Colonel John Boyd, which posits that actors who process this cycle more quickly than their opponent can "get inside" the opponent's decision cycle and gain the advantage.

TO&E: Table of Organization and Equipment. The specified organization, staffing, and equipment of a military unit.

WATCHCON: Watch Condition. An alert posture employed by the DWN.

WMD: Weapons of Mass Destruction

USSR: Former **Union of Soviet Socialist Republics**

The Challenge of Exploring Warning

Problem Statement

Warning is the IC's core—if not preeminent—mission. IC agencies collect and analyze information and disseminate intelligence analytic products inherently to warn key policymakers and decisionmakers across the US Government. Warning's centrality to intelligence is demonstrated by the frequent equating of "intelligence failure" with failure to warn.[5, 6] Thus, advancing the study of warning and proposing new ideas for how to better conceptualize and understand warning can improve the IC's performance writ large. More specifically, improved warning reduces the incidence or impact of surprise[7, 8] and preserves "decision space"[9] for decisionmakers at all levels of government.

Despite this centrality, warning as a specific intelligence discipline and field of study remains underdeveloped—with unexplored concepts, insufficiently defined terms, static approaches, unresolved debates, and common wisdom that has not been sufficiently challenged. Most important, warning lacks a detailed, underlying theoretical framework.

This dilemma is not exclusive to the IC. One scholar observed that "across and sometimes within the intelligence and peace studies literatures, there is no shared understanding of what warning is or should be and how one can best measure its success."[10] This is not the result of the IC's inattention. It has continually worked to improve warning performance through formal studies, symposiums, independent scholarship, and initiatives. A RAND study from 2018 noted that IC efforts to diagnose and remedy problems of warning have established, decarded, and, in some cases, reestablished various roles, responsibilities, or guidance for the warning function.[11] This uneven approach has created a warning mission that is often reactive rather than forward leaning. Without an agreed-upon lexicon, individuals and agencies can end up talking past one another rather than substantively advancing a community debate.

Without a detailed theoretical framework of warning, the IC lacks the common ground needed to advance debate and strengthen capabilities. Creating such a common ground is necessary to improve IC performance. During a workshop on warning hosted by NIU in 2023, a repeated refrain was the difficulty in improving warning or working across IC organizations without a common and more complete understanding of the mission.[12]

Research Questions

Primary:

How does the IC understand warning in the context of its overall intelligence mission, and does this understanding imply that warning is a unique or distinct element of that mission?

Secondary:

What are the theoretically significant concepts and definitions that form the basis of a positive theory of warning?

Purpose and Structure

The overarching purpose of this *Monograph* is to add to the academic and practitioner literature on warning by establishing a research- and data-based foundational lexicon and theory of warning and to inspire informed debate in the IC. The Italian Renaissance saw massive advances in both the arts and sciences, and this work similarly seeks to approach warning as both an art and a science. Warning practitioners sometimes argue, "It's an art and not a science"—a retort also heard in discussions about analysis or intelligence as a profession. At some level, however, all art is based in science. Consider some of the greatest works of Renaissance art, such as Raphael's painting, *The School of Athens* (see Fig. 1). Raphael, Brunelleschi, and other Italian artists used their art to explore and develop drawing in perspective, a technique grounded in the mathematics of geometry and the extended Euclidian plane, as well as the study of optics.[13] Science underlies much in this masterpiece, yet the totality of the work comes together with a certain essence that can only be described as art.

While there is much art in warning, a core tenet of this *Monograph* is that we can explore warning through the underlying lens of science. The use of grounded theory, as a more rigorous, academic method of exploration and analysis, is one way in which this work aims to do so. Additionally, developing formal models for concepts creates a more scientific foundation for how we think about warning and intelligence. Approaching warning from this perspective continues the trend of more rigorous and social-science based explorations of intelligence as exemplified by scholars Erik Dahl,[14] Rose McDermott and Uri Bar-Joseph,[15] and Christoph Meyer et al.[16]

This *Monograph* is divided into two parts:

1. The first addresses the two research questions listed above, using grounded theory to identify the core theoretical concepts needed to create a foundational theory of warning. A review of the most relevant literature on warning identifies key gaps in understanding. Discussions of methodology and research design explore why adopting a constructivist-grounded theory approach to data analysis is beneficial. The data analysis identifies seven theoretical principles of warning to form the core building blocks of a foundational theory of warning.

2. The second integrates these seven principles to create a core lexicon and framework of warning that forms the basis of a foundational theory of warning. These include an initial definition of a threat and two models that create the foundation for conceptualizing warning functions. A framework of warning is then established that consists of four functions: exploratory warning, transition warning, dynamic warning, and explicit warning. Finally, opportunities for future research are explored, as are the implications of the theory for critical debates within the warning literature.

Figure 1. The School of Athens

Raphael, The School of Athens, 1509-11, wikimedia, accessed 8-29-2023. EEPD-199633.

This page is intentionally left blank.

The Intellectual Landscape of Warning

Origins of the Literature and Seminal Works in Warning

The attack on Pearl Harbor in 1941 was not just a catalyst for the development of the IC. It also drove new approaches to consider warning as a distinct intelligence discipline. Warning's objective was to ensure US military and civilian leaders were never again surprised in such a dramatic fashion. The literature on warning that has since accumulated arose from intelligence practitioners rather than academics—with policies, manuals, procedures, and reflections dominating the landscape.

Within the broader literature of intelligence studies, two major works on warning merit special recognition as seminal pieces for their overall impact or scope. The first is Cynthia Grabo's *Handbook of Warning Intelligence,* which stands out as the most comprehensive work on warning's nature and the specifics of warning analysis.[17] Despite its Cold War focus on assessing and warning about military attacks by and engagements with the former Union of Soviet Socialist Republics (USSR), Grabo's work—fully declassified and published decades after its origin in the 1960s/early 1970s—remains a relevant overview and analytic guide. The second seminal work is John Gentry's and Joseph Gordon's *Strategic Warning Intelligence: History, Challenges, and Prospects.*[18] Gentry and Gordon, like Grabo, describe the nature of warning and its many related analytic issues more comprehensively than other modern scholarly works on warning. Their central thesis, however, advocates—or warns—against what they label the "every analyst is a warning analyst" (EAAWA) model and the removal of a dedicated National Intelligence Officer for Warning (NIO/W) from the NIC. Thus, they focus less on analysis and more on the history of warning organizations in the United States and allied nations since World War II. The remaining literature explores more specific or tangential issues and does not match the depth and breadth of these key works.

Differentiating Warning

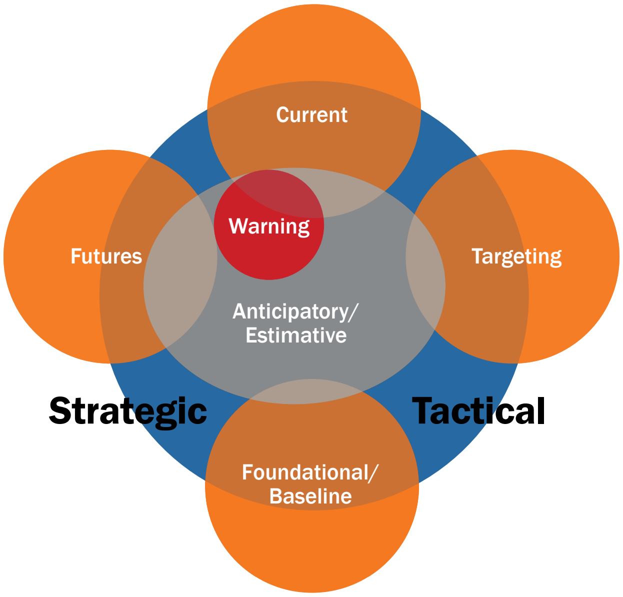
Studying warning requires an understanding of where it fits in the overall sphere of intelligence. Key questions on this topic include "is warning a distinct discipline" and, if so, "what distinguishes warning from other forms or disciplines of intelligence?"

Warning as a Distinct Discipline or Form of Intelligence

Several works that attempt to directly answer these questions fall within the broader literature on intelligence and the ways in which scholars or practitioners organize its missions, functions, and roles. Within this broader literature, warning is most often seen as a distinct form or product of intelligence. The Department of Defense's (DoD) Joint Publication 2-0 (JP 2-0): Joint Intelligence identifies it as the first of eight all-source intelligence product categories,[19] and Robert Clark distinguishes it as one of three types of intelligence products.[20] Both the JP 2.0 and Clark directly contrast "current intelligence" and warning, reinforcing the idea that warning is distinct, yet always in danger of being subsumed by current intelligence. This concern about warning being overshadowed by current intelligence originated with Grabo[21] and Euan Davis,[22] and was reiterated by Mark Lowenthal[23] and Gentry.[24] Gentry and Gordon consider warning to be one of four core intelligence functions, alongside strategic, current, and estimative intelligence.[25] Other authors take a more nuanced view, noting that warning should focus on broader, more strategic issues while acknowledging that current intelligence has a potential role in more tactical warning.[26, 27]

Not all authors or organizations view warning as a distinct intelligence product. The 2019 National Intelligence Strategy (NIS) lists strategic, anticipatory, and current operations intelligence as three foundational missions of the IC, alongside four topical missions. Warning is not called out as a specific discipline, but the sections on strategic and anticipatory intelligence note the need to warn of enduring and emerging threats respectively.[28] For ODNI, warning is arguably an inherent function of both strategic and anticipatory intelligence. Margolis's reconceptualization of the analytic disciplines also presents warning as an inherent function across analytic disciplines.[29] It is worth noting that the 2019 NIS does not directly mention warning in the section on current operations intelligence, mirroring earlier interpretations of tactical warning as the province of operational actors.

Figure 2. DWN Handbook Euler Diagram of Warning.

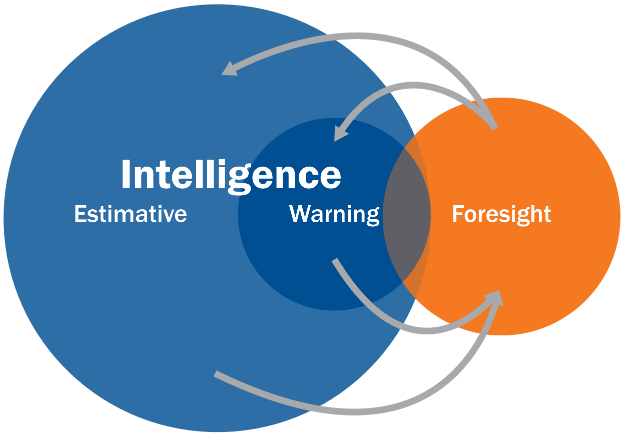


Source: Adapted from DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted material is U.

The increasing use of the term anticipatory intelligence along with enduring and emerging warning over the past decade is relevant because the literature on warning presents two distinct views on what anticipatory intelligence is, each differing in how it relates to or overlaps with warning. The emerging threats school, exemplified by the 2019 NIS, describes anticipatory intelligence as the analysis of "new, emerging trends, changing conditions, and underappreciated developments."[30] This view overlaps with interpretations that equate anticipatory and estimative intelligence, including an interpretation in a previous edition of the *Defense Warning Network (DWN) Handbook* that warning is a subset of anticipatory intelligence.[31]

Similarly, the academic study of foresight includes warning as a subset of estimative intelligence, both of which overlap partially with foresight. (see Fig. 2.) Foresight, however, as described by John Schmidt, usually takes on time horizons and levels of plausibility that extend well beyond that of the IC.[32] (see Fig. 3.) These horizons, taken to the extreme, form the discipline of futures analysis, which intelligence scholars generally consider to be well outside the boundaries of strategic warning or intelligence. Gentry and Gordon, for example, consider strategic warning time horizons to be between six months and two years.[33]

Figure 3. Schmidt Diagram of Warning, Intelligence, and Foresight.



Overlap of analytical strategies between estimative and warning intelligence, and foresight

Source: Adapted from John M. Schmidt, "Intelligence, Strategic Warning, and Foresight: Completing the Package for Decision-Makers," Journal of Intelligence and Analysis, *no. 2 (2015): 11–29.*

The complexity school, however, views anticipatory intelligence as a distinct methodological approach to analysis focused on dealing with the complex systems that increasingly define the international environment. This school, exemplified in the work of Josh Kerbel and drawing heavily from the field of complexity science, argues that today's fundamentally complex strategic environment requires different analytic approaches than the "complicated" environment the IC arguably faced during the Cold War.[34, 35] A critical term in the complexity school is that of "emergent phenomena," which can be defined as new, nonlinear behaviors that arise unpredictably but not entirely unforeseeably, from micro-behaviors in highly interconnected and interdependent systems." The complexity school emphasizes foresight over forecasting, *emergent* threats over *emerging* trends, which could be seen as a contradiction since trends are established patterns and thus, by definition, not emerging,[36] and complex rather than complicated systems.*

Gentry and Gordon do consider anticipatory intelligence under their "other warning techniques" chapter, although their interpretation is heavily influenced by their aversion to the notion of warning as an inherent task of all intelligence analysts (see EAAWA below) rather than a distinct intelligence discipline. Dismissing the term, they contend that the concept "damages the strategic function."[37]

Warning as a Mindset

Instead of focusing exclusively on products or processes, other authors and organizations on both sides of the "distinct discipline debate" consider that the mindset element of warning separates it from other intelligence

* To differentiate between the emerging threats and complexity schools, this *Research Monograph* uses "emergence" and "emergent" in the context of the larger literature on complexity science, and "emerging" warning or threats in the IC's current view of the term.

activities. For Grabo, this meant putting incoming information into a broader, historical context as part of warning's intense research attribute.[38] Among other authors, four distinct elements appear to separate warning from other disciplines: the detection of anomalies, a presumption of and focus on surprise, the consideration of what is possible rather than most probable, and the imperative to convince decisionmakers to act. Anomaly detection, or identifying discontinuities,[39] looks for deviations from established baselines.[40] The *DWN Handbook's* procedures for developing indicators emphasize clearly delineating a baseline or "statement of normalcy" as part of its methodology.[41] Surprise and, more important, preventing it, are hallmarks of the DWN's methodology[42] and definitions of warning.[43] Others noted that warning must presume that surprises will occur.[44] The notion of focusing on what is possible over what is probable is one of the most widely expressed ideas in the warning literature. The *DWN Handbook* notes that warning considers "possibilities over probabilities," while others advised "widen the bounds of the imaginable" [45] or focus on emerging issues.[46, 47] A 1992 Director of Central Intelligence (DCI) Task Force report on warning noted that, while all analysts might follow the same fundamental process, warning analysts succeed in identifying threatening developments is because they "approach the problem with the objective of doing so, and other analysts most often do not."[48]

The Imperative To Convince or Persuade

Another attribute of warning in the literature is an imperative to convince decisionmakers as part of a warning-response dynamic. Warnings bear an importance different from other intelligence assessments and communications and are not successful until they have had sufficient impact. Earlier authors noted that consumers must "know they have been warned,"[49] and need to be informed "recently, and with sufficient evidence to make it stick."[50] Gentry notes intelligence failures can result when warnings are presented "unpersuasively"[51] and, with Gordon, defined strategic warning partially as "convincing [decisionmakers] that unpleasant and costly measures may need to be taken in response" to threats. Other authors have emphasized persuasion in warning messages; even Grabo has been quoted as saying "warning is useless unless it results in action to forestall disaster."[52] Meyer et al. go further, establishing a full "theory of conflict warning as persuasion in foreign policy" and looking at warnings that emerge from within organizations and states and those that come from external nongovernmental organizations, which they label as "inside-up" and "outside-in" persuasion, respectively.[53] The one quasi-counter to this perspective comes from the *DWN Handbook,* which notes that successful warning should enable a decision—including a decision not to act.

The dominant view in the literature, however, is that a warning is successful only when it is convincing, persuasive, or detailed enough to enable preventative action against a threat.[54] Some authors looked at this dynamic from the perspective of the decisionmaker, asking instead why some accurate or prescient warnings are not heeded. Richard A. Clarke and R. P. Eddy create a "Cassandra Coefficient," noting four factors that can result in unheeded warnings: the warning itself, the decisionmakers, the predictor (or possible Cassandra), and critics of the warning.[55] They note that when these factors are taken into account, decisionmakers can possibly avoid dismissing relevant warnings, but the authors do not directly address how to make warnings more convincing.[56] Michele Wucker expanded on this dynamic by developing the notion of a gray rhino—a highly probable but ignored threat—and exploring why decisionmakers fail to take preventative action in spite of "obvious threats" and warnings.[57]

The dynamic between intelligence and decisionmakers, particularly the emphasis on persuasion, is important because it is a core tenet of intelligence, at least in Western nations, that intelligence should remain apolitical and not recommend policy. To be successful, however, warning requires a convincing and persuasive argument that results in action, so intelligence warnings are de facto advocating for a specific policy or decision. Few authors have addressed this within the literature specifically addressing warning.[†] The CIA's Jack Davis recommended a collaborative relationship and improving analysts' understanding of the policy environment as a means to better craft warnings.[58] Betts addressed the separation of intelligence failure from policy failure, stating that "the personnel can be segregated, but the functions cannot,"[59] while Gentry recommended reframing intelligence failure as a national security failure.[60] In his exploration of warning of the COVID-19 pandemic, Dahl acknowledged the delicate balancing act intelligence must perform but cautioned against setting the bar for warning success too low. He argued that "analysts can and must be ready to push harder if they feel their warnings are not being heard."[61] The question of when the bar is set too high is left unresolved.

Resolving the overall question of where to set the bar for warning success could be considered a potential gap in the literature on warning. If success means that an action is taken to preempt, prevent, or prepare for a threat, then does successful warning imply that the IC is advocating for action, even if not a specific course of action? After all, a failure to persuade a decisionmaker leaves the IC open to the retort reputedly issued by former National Security Advisor Henry Kissinger, "You warned me, but you didn't convince me."[62]

Defining Warning

Core Themes

One of the most troublesome areas of warning scholarship and practice has been establishing a common lexicon, making definitions one of the most important elements within the literature on warning. The difficulty in defining what warning is and distinguishing it from other intelligence missions or products might be explained both by the broad ways in which the term can be interpreted and the diverse perspectives of IC components and scholars interpreting it. Indeed, Grabo dedicated two chapters in *Handbook of Warning Intelligence* to describing what warning is and is not. Much of her emphasis is on the analytic nature of warning, stating that warning "is not a commodity. Warning is an intangible, an abstraction, a theory, a deduction, a perception, a belief. It is the product of reasoning or of logic, a hypothesis whose validity can be neither confirmed nor refuted until it is too late."[63]

Authors who have attempted to write a singular definition of warning often focus on one or more central themes. DCI Directive (DCID) No. 1/5, *National Intelligence Warning,* defined warning as "those measures taken, and the intelligence information produced, by the Intelligence Community to avoid surprise to the President, the NSC, and the Armed Forces of the United States," emphasizing warning's mission is to avoid surprise.[64] DoD, through policy documents and several versions of the *DWN Handbook,* emphasizes warning as a communication, most recently defining it as "a distinct communication to a decisionmaker about threats

[†] A full accounting of the extensive literature on the relationship between policy and intelligence is outside the scope of this study.

against US and allied security, military, political, information, or economic interests."[65, 66, 67, 68, 69, 70] Meyer et al. define warning purely as a communication, stating that it is "a single or a series of closely coordinated communicative acts by a given persuader intended to raise the awareness among one or more persuadees for an impending threat to a valued good."[71]

The timing of a warning's communication is also a central theme among the many definitions. The DWN definition specifies that "The message should be given in sufficient time to provide the decisionmaker opportunities to avoid or mitigate the impact of the threat." Other DoD and DoD-affiliated publications define warning along this theme, describing warning as "timesensitive [sic] intelligence information on foreign developments that forewarn of hostile actions or intention,"[72] or "a notification of *impending* [emphasis added] activities that may, or may be perceived to, adversely affect US national security interests or military forces."[73]

Another theme in the DWN definition, damage mitigation, is echoed by other intelligence scholars, such as Davis, who argue warning analysis "seeks to *prevent or limit* damage [emphasis added] to US national security interests via communication of timely, convincing, and decision-enhancing assessments that assist policy officials to effect defensive and preemptive measures against future threats and to take action to defend against imminent threats." Davis's characterization of warning is perhaps the only definition that distinguishes between future and immediate threats—the key factor distinguishing the two commonly used terms in the warning literature: strategic and tactical warning.

The Strategic/Tactical Paradigm

If a dominant paradigm exists in the intelligence warning literature, it is the division of warning into strategic and tactical domains. Strategic warning often acts as the overall definition of warning, while tactical warning is dismissed as a military or operational concern.[74] Grabo defined strategic warning as "an assessment that the enemy has or probably has taken a decision to employ force," distinguishing between probability and imminence. For Grabo, tactical warning was "not a function of intelligence (at least not at the national level) but is an operational problem." Most differentiations between strategic and tactical warning define strategic warnings as coming before an attack. Tactical warnings are those issued about an "imminent"[‡] attack or after an attack has begun, but before weapons have impacted, such as missiles or bombers in flight.[75, 76, 77, 78, 79] Ultimately, this interpretation of warning derives from the Cold War's defining challenge, providing warning of a sudden conventional or nuclear attack from the former USSR using intercontinental ballistic missiles or strategic bombers. Academics Uri Bar-Joseph and Rose McDermott provide a different interpretation; they argue strategic warning has two functions that blend what others break out between strategic and tactical. To them, strategic warning's first task is "to inform policymakers that their deterrence strategy has ceased to be effective," while the second "is to provide a high-quality warning before the actual attack takes place."[80]

While the strategic/tactical dichotomy is arguably the dominant view of warning, other authors offered different interpretations of what constitutes strategic warning. As mentioned before, Davis used a broad versus

[‡] Imminence is also not well defined in the literature and is referenced both in temporal terms (minutes, hours, or days before an event) and in terms of probability. That debate is beyond the scope of this study.

specific differentiation, arguing that "strategic warning addresses perceived dangers in broader terms," while tactical warning "seeks to detect and deter specific threats to US interests" to "avoid incident surprise and thus block or blunt damage." Other conceptualizations of strategic warning emphasized the level of the decisionmaker (typically the president or national leadership),[81, 82] the nature of the threat,[83] or the availability of resources to respond to a threat.[84]

Given the existence of the operational level of war between the strategic and tactical levels within US military doctrine, some DoD entities and authors formed definitions for operational warning, which in some cases is equated with operational commands or operational plans.[85, 86] Another interpretation is that of a middle link between strategic and tactical timelines.[87, 88]

Emerging, Enduring, and Political Warning

DoD, through the DWN, also distinguishes between emerging and enduring threats that somewhat parallel Davis's broad versus specific distinction, although these differentiate more on ambiguous versus well-defined threats. For the DWN, emerging warning provides monitoring of "newly identified issues relevant to national security of sufficient significance to warrant temporary attention by the Defense Intelligence Enterprise," and warning on enduring threats addresses a "significant national security issue, usually linked to an operation plan or concept plan, that is well defined, and longstanding potential threats to the interests of the US [sic] and its allies." These definitions create emerging or enduring "warning problems"—named issues or threats that analysts monitor.[89]

Finally, Grabo's idea of political warning refers to assessing the intent of potential adversaries.[90] The term was defined more formally by at least one publication, but it is not prevalent enough in the literature to be considered a full part of the lexicon.[91]

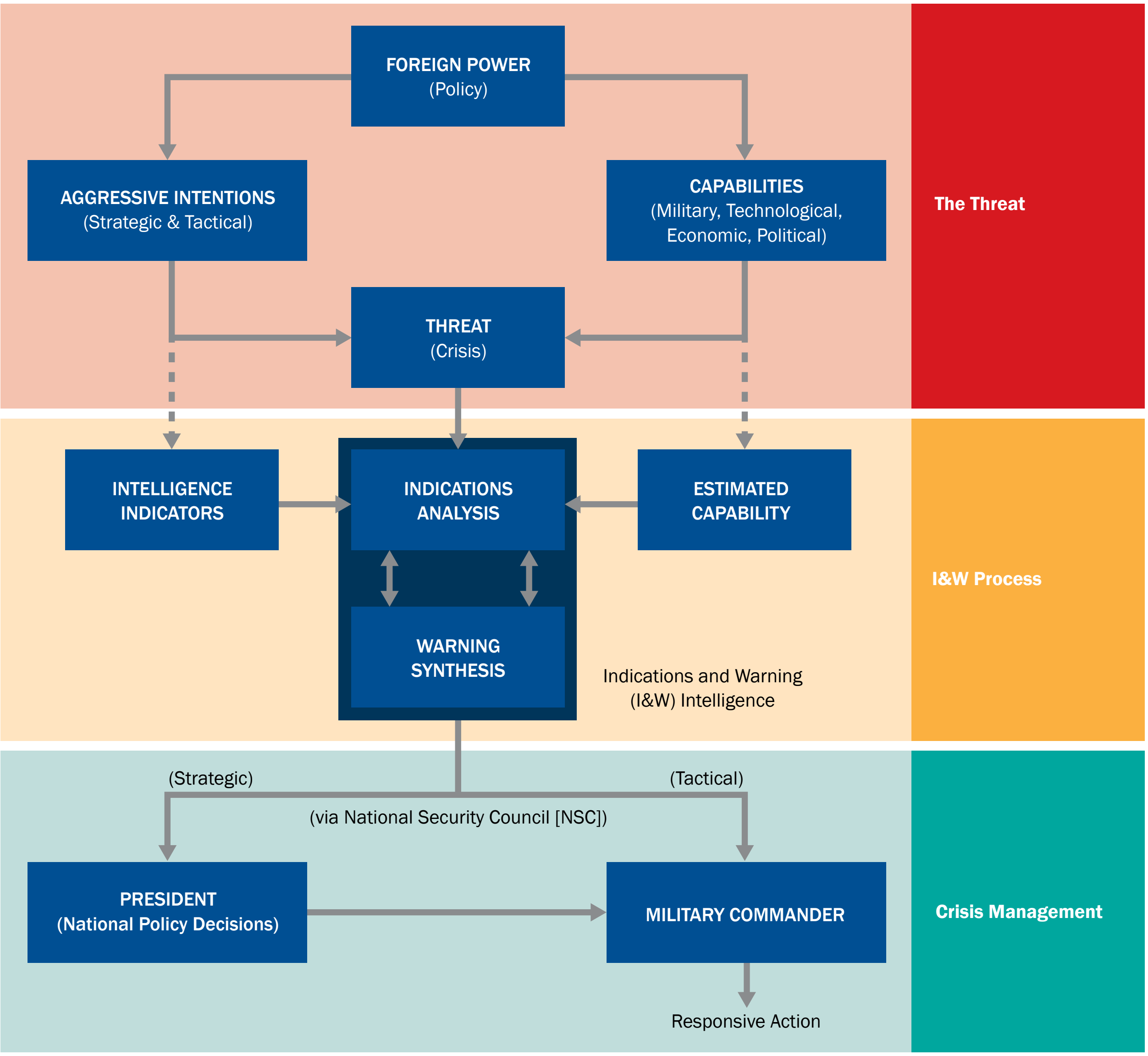
Warning as a Process

Outside of formal definitions, the most common conceptualization of warning is that of an analytic process. The DWN and its predecessors employ the most formal process-based model of warning, detailing processes for establishing and monitoring warning problems, especially in earlier editions of the *DWN Handbook,*[92, 93] with a focus on the procedural steps for assessing or exploring an identified issue rather than on warning as a general discipline. A CIA exploration of warning provides a more comprehensive, theoretical process starting with the emergence of a threat and the subsequent signals to be collected, analyzed, and communicated to decisionmakers, so they can determine how to react and deal with any counteractions. This overview of warning uses the analogy of a "fragile chain of warning" to represent how a breakdown at any step can lead to failure.[94] The CIA's treatment is arguably the most thorough process description within the IC, reflecting process outlines by Betts[95] and Gentry,[96] although Gentry includes an additional step at the beginning for strategic planning on the part of IC collectors and policymakers. Gentry's strategy step may be instrumental in determining the IC's ability to collect and to recognize the weak signals that initiate the CIA process model.

Models of Warning

Most visualizations of the warning mission either provide graphic depictions of the process,[97] or Euler diagrams showing where warning overlaps or is separate from other intelligence functions (see "Differentiating Warning" above). Two works, however, use a model to place warning in a more theoretical context. The first is an early primer on warning developed for the Defense Intelligence School (a forerunner of NIU), which depicts the "Indications and Warning (I&W) Process" as an intermediary element between threats and crisis management (See Fig 4.).

Figure 4. An Early Model of Warning.

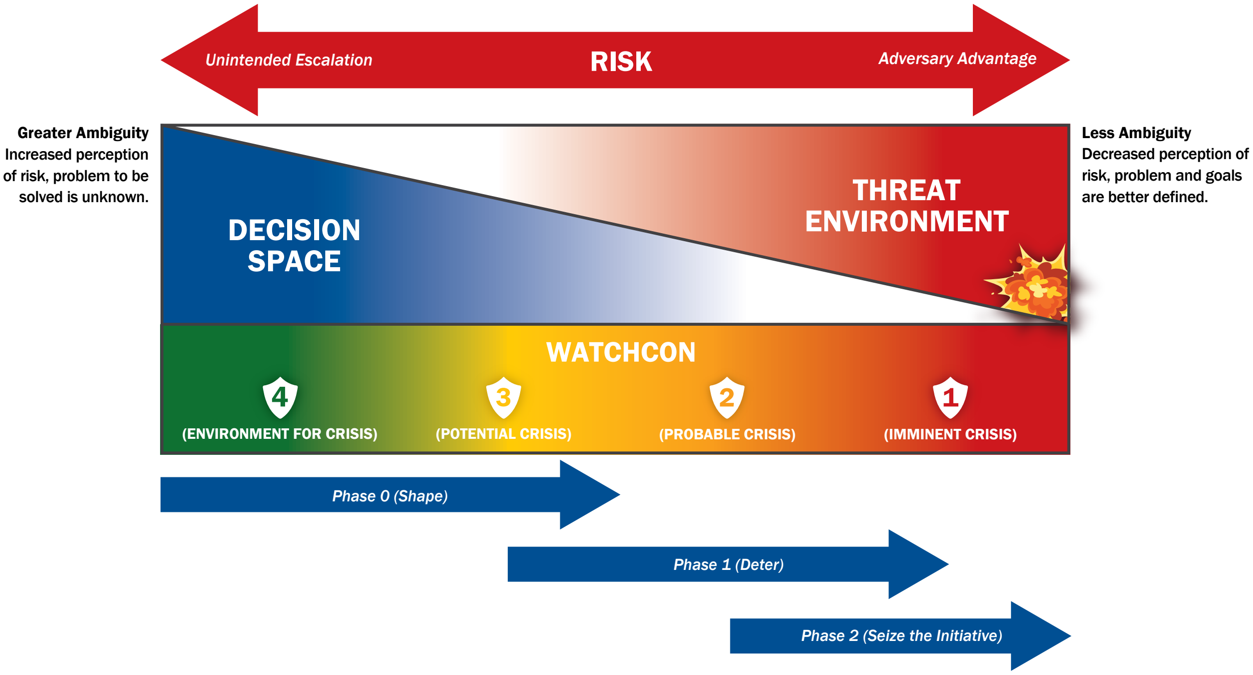


Source: Adapted from SCITEK, (U) Indications and Warning Intelligence *(Washington, DC: Defense Intelligence School, 1974): 1–6, Classification of extracted material is UNCLASSIFIED.*

Within this model, indicators and capability assessments come together in indications analysis to provide warning to national civilian and military decisionmakers.[98] This model uses the decisionmaker as the distinguishing factor between strategic and tactical warning, with strategic warning directed toward the president for national policy decisions and tactical warning directed toward miliary commanders who take responsive action.

More recent editions of the *DWN Handbook* present a unique model of warning as a means of preserving decision space for national leadership as threats develop and come to fruition. In this model, as a threat becomes more likely and less ambiguous, the time and space for preventative or preemptive decisions shrinks. (See Fig 5.) Through distinct warnings—or Watch Conditions (WATCHCONs)—at various points in the timeline, intelligence ensures decisionmakers remain aware of the shrinking decision space.[99]

Figure 5. The DWN Decision Space Model of Warning.



Source: Adapted from DOD Inspector General (IG); DODIG-2020-055; January 30, 2020; "(U) Evaluation of US European Command's Warning Intelligence Capabilities," (Redacted); Classification of extracted material is U; Overall classification is U. https://www.oversight.gov/report/dod/evaluation-us-european-commands-warning-intelligence-capabilities.

Threats: Capability and Intent

Although several writings on warning emphasize including opportunities to counter threats, the overriding focus is on identifying and characterizing those threats. When discussing threats, the dominant paradigm in both warning and general intelligence analysis literature is that a threat combines capability and intent. Gentry and Gordon note this dominant view, stating that "if there is any truism in military intelligence, it is that threats are composed of capabilities and hostile intentions."[100] In discussing threats in these terms, Grabo devotes more time to intent than capability, contending that "warning has failed more often for lack of political perception than it has for military evidence."[101] The 1992 DCI Task Force report also recognizes the difficulty associated with warning based on intent, stating that "it often hinges on assessments of intentions, on the specific moves contemplated by a foreign principal during complex situations. Often the foreign principal's intentions are not fixed during the formulative stages of a crisis situation. Hence, intelligence cannot easily anticipate decisions that the subject actors themselves have not yet made." The challenge of shifting intentions is noted repeatedly in the literature on intelligence failure and the inevitability of surprise (see "Warning-Adjacent" Literature below).[102]

This might lead to the conclusion that warnings based on capability are not as difficult, but assessing capabilities has its own set of challenges, which Grabo acknowledges in noting that "nearly all Western nations at some time or another have been victims of gross misjudgment not only of the intentions *but of the capabilities of other powers* [emphasis added]."[103] When it comes to tradeoffs between assessments of capabilities and intentions, Grabo and others conclude that warning and planning based on known capabilities is likely to reduce the incidence of surprise.[104] According to Michael Handel, "in the final analysis, it is always safer to gear one's plans more to the capabilities of the enemy than to his intentions."[105]

Overall, the capabilities-plus-intent conceptualization of a threat still dominates more contemporary writings, but as the overall scope of threats the IC considers has increased, some authors have noted deficiencies with the idea. Lowenthal notes that "cyberspace appears to upset many of the strategic early warning concepts familiar to us. Intentions are not any more or less opaque than before, but the issue of capabilities has basically disappeared."[106] Furthermore, the complexity school of anticipatory intelligence (see Differentiating Warning above) explicitly argues that complex systems can see behaviors arise without a distinct intent, necessitating foresight over forecasting and holistic over reductionist practices.[107] Although some attempts to consider complexity and ambiguity in warning gave rise to the DWN's definition of emerging warning, relatively little formal scholarship exists on the potential shortfalls of the indicators and scenarios methods.

Organizing the Mission

The academic literature gives relatively little attention to how nations organize themselves to execute the warning mission, with the notable exception of Gentry and Gordon who provide both an in-depth history of US and Allied warning institutions and develop a typology of organizations.[108] They list the following six organizational schemes across history:

1. National leaders as warning analysts,
2. All analysts are warning analysts (the EAAWA model),
3. Separate organizations responsible for warning,
4. Hybrid warning organizations,
5. Whole-of-government warning systems, and
6. No warning organization (that is, no effective intelligence system).

Along with several other attributes of US intelligence warning, Gentry and Gordon criticize the EAAWA model, which they assert the IC has used since the elimination of an NIO/W and an independent warning deputy within the Joint Staff Directorate of Intelligence (JS J2).[109] Other authors who address the topic either describe how certain entities have set up their system,[110] detail specific procedures and responsibilities within warning systems (namely DoD structures),[111, 112] or issue direct guidance to IC elements.[113, 114]

Time and Timing

As mentioned, (see Defining Warning above) one theme that permeates the literature on warning is that of time and the timing of warnings. All components of the literature agree that any successful warning must be delivered in time for policymakers or operators to take policy, planning, or operational actions. The discussion is slightly more varied or complicated, however, regarding the tradeoffs between warning too early or too late. Reginald Jones, often credited as the father of technical intelligence in WWII, noted that intelligence must "bark at the right time" and identified the two most well-discussed implications of this challenge.[115] Sound the alarm before evidence is sufficient for a confident assessment, and the IC runs the risk of a false positive that does not emerge—known as the "boy who cried wolf" phenomenon,[116] cry wolf syndrome,[117] or other "cry wolf" phrases.[118, 119, 120] On the contrary, barking too late reflects a desire to wait for more information to reduce uncertainty and ambiguity. Regarding this dilemma, Clark noted that a "false alarm will normally be overlooked or forgiven much more easily than a failure to call the shot on something that does happen,"[121] but others have noted that either error can be damaging[122] or that repeated false alarms can dull intelligence and policymakers' reactions.[123]

Warning and Analysis

Structured Techniques. Although most DoD elements define warning as "a communication," the discussion on warning is largely connected to the specific analytic techniques relevant to warning. This branch of the warning literature overlaps with the broader literature on analysis and structured analytic techniques, most of which are beyond the scope of this study. Two major elements of the literature on structured techniques, however, do merit inclusion: indicators and scenarios.

Indicators and indicator lists are the core structured technique for warning, so much so that the term "indications and warning" was prevalent in DoD terminology for several years before being removed from joint publications to reduce confusion and inconsistencies.[124, 125] The use of indicators was pioneered during the early days of a formal warning structure in US intelligence. Grabo detailed specific types of indicators and considerations for them.[126] Although both the IC and nonintelligence organizations reference indicators and indicator lists,[127] their use was most prevalent within DoD and the DWN, which established precise procedures for developing, evaluating, and displaying indicators.[128, 129] Indicators are central to warning based on the idea that observable events or signatures must happen, or are highly expected to happen, before a threat occurs.[130] These observables allow intelligence organizations to detect and more accurately assess when a threat becomes more likely or is about to occur. Several authors proposed criteria for what makes a good indicator, and their lists largely converge on six core elements: indicators must be timely, observable, valid, reliable, stable, and unique.[131, 132, 133, 134]

Scenarios, the second major structured technique applicable to warning, have two major uses. First, scenarios are used after a singular threat has been identified to help develop indicators.[135, 136] For the CIA and other agencies, however, scenarios are used as an inductive analytic exercise to discover possible threats as an analysis of alternatives approach, going so far as to define strategic warning as a branch of alternative analysis.[137]

The "Warning-Adjacent" Literature

One difficulty in reviewing and assessing the literature on warning is that the broad scope of the warning mission means that several other fields of study, each with their own deep literature, can overlap with that of warning. To make the overall task more manageable, this study refers to these fields as the "warning-adjacent" literature. Four adjacent fields merit discussion: intelligence success and failure, surprise, cognitive science, and individual disciplines.

Intelligence Failure (and Success?)

Intelligence failure (or intelligence success and failure as it is arguably evolving into) overlaps with warning to the greatest degree and, as mentioned earlier, is sometimes used synonymously with a failure to warn. Most case studies focus on the failure to assess or prepare against surprise attacks such as Pearl Harbor, the Yom Kippur War, the Korean War, or Iraq's invasion of Kuwait.[138] Much of this literature focuses on in-depth reviews of a single case. Two of the most notable are the seminal warning case studies by Roberta Wohlstetter on Pearl Harbor[139] and the 9/11 Commission Report,[140] which popularized the euphemisms "filtering the signal from the noise" and "connecting the dots," respectively. Additionally, the past decade has seen a rise in integrating more rigorous social science methods into comparative case studies exemplified by Dahl[141] and Bar-Joseph and McDermott.[142] The first focuses on identifying and testing the effects of causal variables such as receptivity, and the second on individual learning.

Theories on why intelligence fails identified the following: 1) the failure to correctly assess adversary intentions (which overlaps the broader literature on analysis, biases, and mindsets),[143] 2) individual versus organizational explanations,[144] 3) lack of decisionmaker trust and receptiveness to intelligence,[145] and 4) analytic revisionism.[146] Recently, however, some scholars have begun to explore a gap in that literature: intelligence success. The origin of this newer field owes much to studies by Robert Jervis, and it includes explanatory variables such as personal learning from past failures.[147]

Other explorations of intelligence failure have focused on the inevitability of surprise as a natural occurrence that can be minimized, but not eliminated, citing factors that make forecasting and world events inherently vulnerable to ambiguity, misperception, and variation in behavior.[148, 149, 150, 151, 152] Among the many authors contributing to this field, Richard Betts authored the seminal studies most often cited. Meanwhile, Gentry proposes a reframing of intelligence failure as national security failure, establishing six types of national failure to include traditional intelligence failures, but also failures by policymakers to respond to valid warnings. Gentry's list of failure types is notable for including failures to warn or respond to warnings about opportunities.[153]

Of primary interest to this study is the analysis of warning success and failure, specifically the topic of success, in contrast to broader exploration of intelligence success and failure. Detailed explorations of success in intelligence are a major gap, and while Bar-Joseph and McDermott present an explanatory variable in personal learning, their use of comparative case studies does not account for original failures, only the causal effect of individual learning.[154] Thus, their variable cannot adequately explain or illuminate the first case in each dyad they explore.

Surprise and Intelligence Failure

Although the literature on intelligence failure and success arguably deals with surprises, particularly surprise attacks, additional literature looks at the phenomena of surprise more directly. The seminal exploration of this field is Ephraim Kahn's exploration of surprise attacks, which addresses the elements of surprise attack, including warning concepts and assessments of intention and capability, intelligence analysis, and the organizational context in which intelligence and decisionmaking occurs.[155] Ariel Levite provides one of the simplest, yet most powerful definitions of surprise—"the sudden realization that one has been operating on the basis of an erroneous threat perception."[156]

One of the most unique and useful studies on surprise in intelligence is the typology of surprise developed by Michael H., which goes beyond the literature on intelligence failure by classifying the types of events that surprise us.[157] He identifies three major categories: sudden hostile action, system shock, and tectonic shifts.

Cognitive Sciences

Intelligence analysis's overlap with the psychology of processing and making sense of information—-as well as responding to warnings and deciding whether to act—connects the full field of cognitive sciences to warning. Notable contributions with special relevance include Nassim Taleb's[158] idea of the black swan, Wucker's gray rhino,[159] and Daniel Kahneman's systems of thinking.[160] Finally, Richards Heuer explores the general psychology of intelligence analysis in his seminal work on the topic.[161]

Specific Discipline Studies

Within the domain of warning, some studies have looked at the specific details, indicators, and nature of warning for different types of threats. These disciplines can include military threats, state instability, demographic shifts, economic threats, and genocide warning.[§] Cyber threats have been a particularly significant

[§] For a review of these topics, Gentry and Gordon provide the most comprehensive overview in *Strategic Warning Intelligence.* Part of what makes this book so important to warning, especially contemporary warning, is the breadth of issues they explore and the challenges to what they view as strategic warning.

area of study, including Gentry's work, which seeks to show how strategic warning is possible in a field often seen as highly tactical given instantaneous time horizons for an attack.[162] ¶

Major Gaps and Findings

Two major weaknesses in the literature on warning are notable. The first is the lack of a core framework and sufficiently theoretical model of warning. Most warning frameworks are simply processes, and the two arguably theoretical frameworks from the Defense Intelligence School and DWN do not adequately illuminate all core themes and concepts from the literature on warning. The lack of a solid theoretical framework has allowed for wild variations in how scholars and practitioners define core terms—warning, strategic warning, tactical warning, decision space, and so forth. The dominant paradigm of the strategic/tactical dichotomy is more likely the result of a path-dependent evolution from the origins of the IC through the Cold War and beyond, rather than the development of an academic discipline. As such, it needs to be challenged to determine if reframing and redefining terms can provide a substantively better solution.

Second, the central concept of threat as "capability plus intent" is insufficient for today's international environment and the scope of concerns facing US senior decisionmakers. In addition to the challenges in assessing intent identified in the literature, the notion of intent is insufficient or inappropriate for a wide swath of current US national security concerns. Intent requires individual decisionmakers to have control over organizational or national courses of action, which only applies to one of the three categories of Michael H.'s typology of surprise: sudden hostile action.[163] The other two categories, system shock and tectonic shifts, arise from conditions of complexity and require metaphors or models from complexity science. Those metaphors focus on when conditions are ripe for action or surprise,[164] not on specific predictions about the timing of an event.

This *Monograph* adds to the literature on warning by addressing the first gap directly, and the second gap indirectly.

¶ These individual discipline-based explorations of warning fall outside the scope of this study.

A Constructivist Grounded Theory Approach to Warning

Conceptual Framework

As discussed in the previous section, one challenge in studying warning is the lack of a theoretical or conceptual framework that covers the entirety of the mission and the key themes contained within the literature. Thus, one of the major objectives of this research is to develop such a framework.

The underlying theoretical framework for this project is constructivist theory (or philosophy). The constructivist approach asserts that warning is a social construct of the intelligence and the broader national security communities, and the mission is determined by how we define and conceptualize it. Therefore, the researcher is not attempting to observe and understand an objective reality of warning, but rather is trying to discover how warning has been and is currently constructed by both scholars and practitioners. The existing literature supports this theoretical approach by largely defining and characterizing warning as a process, a communication, or an analytic discipline. The impact of organizational identity on warning can also be seen in the way that DoD's and CIA's views of warning take on aspects of each organization's worldview, such as DoD defining an operational level of warning consistent with its doctrinal construct of three levels of warfare.

Overall Research Methodology

This study employed an exploratory, qualitative approach, using established practices from grounded theory, to build a conceptual framework of warning and explore its characteristics.[165] Grounded theory is an ideal approach—both in its overall philosophy and specific methodology—because a comprehensive theory of warning does not exist and relationships between concepts are not well articulated. More specifically, this study employed constructivist grounded theory (C-GT) as developed and explained by Kathy Charmaz.[166] A constructivist approach was chosen over a positivist approach for several reasons. First, as stated above, this study views warning as a social construct. Its definitions, terms, and overall conceptualization appear to be influenced by an organizational or author background. Viewing warning as a social construct matches the C-GT philosophy that no objective reality exists around the object or phenomenon under study.[167]

Second, a core tenet of C-GT is that the researcher is not a completely impartial observer of the phenomenon under study, but an active participant in theory construction, who is aware of, and influenced by, the established literature. As a former senior analyst for the DWN and having compiled the literature review above, it is unreasonable to assume I have an absolutely impartial stance. This status, however, does present a challenge. One major critique of C-GT is that the approach does not allow for sufficient theoretical sensitivity as compared to a positivist approach. The idea of theoretical sensitivity is critical to grounded theory. It is the sensitivity of a researcher to detect trends, themes, and relationships which emerge from the data. Positivist grounded theory very specifically avoids a major literature review to prevent established views from influencing data analysis. Researchers following the positivist approach should be relative outsiders to the populations under study to maintain a truly impartial view and maximize sensitivity to themes in the data. C-GT, on the other hand, does allow for, and generally conducts, a literature review early in the research process to better frame and focus subsequent phases such as interviewee selection and interview question composition. It also recognizes the benefits to be gained from having at least some background in the phenomena and population under study.[168] This study worked to maintain theoretical sensitivity by incorporating a dataset that represented diverse views on warning and a strict adherence to coding and note-writing practices to ensure derived codes capture the views of study participants and original authors, not those of the researcher.

A second positivist critique of C-GT is that the results cannot be duplicated, because individual observers are not equally impartial and will have different underlying understandings or assumptions. A second researcher, applying the same methodology to the same datasets, would very likely establish a coding framework that differs from the first researcher and thus, potentially, establishes a different theory. Rather than a weakness, however, C-GT theorists see this as a strength, allowing for multiple perspectives and developing a theory by comparing studies whose results differ significantly.[169]

Peer review of research results before publication revealed what could be considered two underlying assumptions about warning that must be acknowledged. First, this study assumes warning is a distinct concept and phenomenon that exists within the field of intelligence and national security. Fully articulating that concept, however, has always been a challenge. The difficulty of the task is exemplified in how Grabo, arguably the most experienced and influential author on warning, attempted to do so. Her description of warning, partially quoted above, is worth repeating in full here:

> *"Warning is not a fact, a tangible substance, a certainty, or a probable hypothesis. It is not something which the finest collection system should be expected to produce full-blown or something which can be delivered to the policy maker with the statement, "Here it is. We have it now." Warning is an intangible, an abstraction, a theory, a deduction, a perception, a belief. It is the product of reasoning or of logic, a hypothesis whose validity can be neither confirmed nor refuted until it is too late."*[170]

This study assumes that warning contains some characteristic(s) that distinguishes it from other analysis and production activities within the IC and the national security enterprise. It does not make assumptions about what that distinction is, however, and any answers provided must be grounded in the data collected.

Data Collection, Generation, and Processing

Data collection and generation occurred in two phases. The first consisted of a review and coding of relevant, available documents conducted simultaneously with the literature review. The second phase, informed by the first, consisted of semistructured background discussions with 11 individuals from across the IC, which were subsequently coded and analyzed. This phase also integrated notes and proceedings from an NIU-sponsored workshop exploring warning. Integrating the workshop discussion notes allowed for a significantly broader sampling of views from IC and law enforcement agencies, doubling the number of expert consultations conducted.

Phase 1: Extant Document Selection and Coding

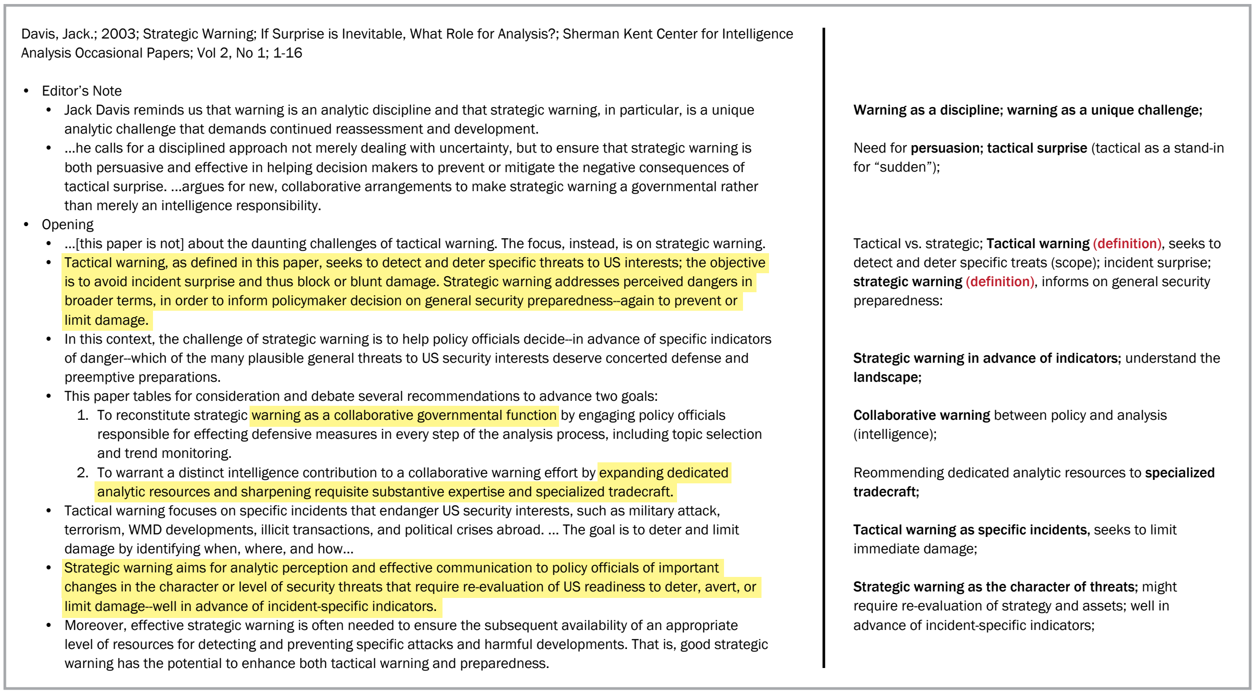
Documents form an important data source for grounded theory research and can consist of extant or elicited documents that include manuals, reflections, and elements of the overall literature.[171] Document analysis was employed in grounded theory studies by J. S. Chen,[172] Helen Hardman,[173] and Glenn Bowen.[174, 175] Furthermore, document analysis in grounded theory helped inform subsequent interview phases as demonstrated by Bowen.[176] As Nicholas Ralph et al. caution, however, distinct differences exist within grounded theory between using data from extant documents and that obtained through observation or interviews. The authors caution that the *data generation* process of interviews or observations differs from the true *data collection* process of extracting codes from documents where they were already there.[177] Thus, coding of extant documents was conducted as a separate phase of research largely ahead of expert consultations and interviews. This approach was adopted to focus the scope of research because views on warning varied widely in the literature. This allowed for more focused interview questions and appropriate theoretical sampling in accordance with grounded theory practices.[178]

Data collection was accomplished by identifying relevant entries from the bibliographies and required readings for classes that were part of the NIU Graduate Certificate in Strategic Warning, from a general search of the academic journal storage (JSTOR) digital library using the search terms "strategic warning" and "warning analysis," from a review of all article titles and summaries for the *Studies in Intelligence* journal (conducted via classified networks to capture articles at all classification levels), and from previously acquired researcher holdings and professional references. This final category of documents was developed over six years working as an instructor for DIA's Warning Analysis Course, as the senior intelligence analyst for the DWN, and as a manager for DWN policy, tradecraft, and training. It allowed for the consideration of hard copies of older and less readily available materials such as the first three versions of the *DWN Handbook.*

In observance of the considerations for use of documents in grounded theory research established by Ralph et al., determination of which documents from the literature review and general data search would be included for coding used a loose form of *contextual positioning* to determine relevance to the central research question.[179] The majority of documents selected for coding form what might be called the "core literature," which deals directly with warning as the central object of study, policy, or discussion. As an example, cited works by Davis concern themselves exclusively with the topic of warning and were included in the coding process. Works cited by Schmidt or Kerbel, which focus on foresight or anticipatory intelligence, respectively, however, were not coded. When considering larger books, only select chapters or sections sufficiently focused on warning or warning-adjacent topics were included. See Appendix A for a complete list of documents selected for coding across all phases.

Initial coding for documents began with reading the full document, such as an article, manual, or book chapter, and identifying the text's most important elements. Initial codes were then called out next to the corresponding text. Then, the focused coding process looked at all initial codes and identified those assessed as most significant by bolding them. Given the importance of identifying varying definitions of key terms, a limited number of codes were called out as definitions. An example of initial and focused coding is provided in Fig. 6.

Figure 6. Initial and Focused Coding Procedure.



Davis, Jack.; 2003; Strategic Warning; If Surprise is Inevitable, What Role for Analysis?; Sherman Kent Center for Intelligence Analysis Occasional Papers; Vol 2, No 1; 1-16

- Editor's Note
  - Jack Davis reminds us that warning is an analytic discipline and that strategic warning, in particular, is a unique analytic challenge that demands continued reassessment and development.
  - ...he calls for a disciplined approach not merely dealing with uncertainty, but to ensure that strategic warning is both persuasive and effective in helping decision makers to prevent or mitigate the negative consequences of tactical surprise. ...argues for new, collaborative arrangements to make strategic warning a governmental rather than merely an intelligence responsibility.
- Opening
  - ...[this paper is not] about the daunting challenges of tactical warning. The focus, instead, is on strategic warning.
  - Tactical warning, as defined in this paper, seeks to detect and deter specific threats to US interests; the objective is to avoid incident surprise and thus block or blunt damage. Strategic warning addresses perceived dangers in broader terms, in order to inform policymaker decision on general security preparedness--again to prevent or limit damage.
  - In this context, the challenge of strategic warning is to help policy officials decide--in advance of specific indicators of danger--which of the many plausible general threats to US security interests deserve concerted defense and preemptive preparations.
  - This paper tables for consideration and debate several recommendations to advance two goals:
    1. To reconstitute strategic warning as a collaborative governmental function by engaging policy officials responsible for effecting defensive measures in every step of the analysis process, including topic selection and trend monitoring.
    2. To warrant a distinct intelligence contribution to a collaborative warning effort by expanding dedicated analytic resources and sharpening requisite substantive expertise and specialized tradecraft.
  - Tactical warning focuses on specific incidents that endanger US security interests, such as military attack, terrorism, WMD developments, illicit transactions, and political crises abroad. ... The goal is to deter and limit damage by identifying when, where, and how...
  - Strategic warning aims for analytic perception and effective communication to policy officials of important changes in the character or level of security threats that require re-evaluation of US readiness to deter, avert, or limit damage--well in advance of incident-specific indicators.
  - Moreover, effective strategic warning is often needed to ensure the subsequent availability of an appropriate level of resources for detecting and preventing specific attacks and harmful developments. That is, good strategic warning has the potential to enhance both tactical warning and preparedness.

Warning as a discipline; warning as a unique challenge;

Need for **persuasion; tactical surprise** (tactical as a stand-in for "sudden");

Tactical vs. strategic; **Tactical warning** (definition), seeks to detect and deter specific treats (scope); incident surprise; **strategic warning** (definition), informs on general security preparedness:

Strategic warning in advance of indicators; understand the **landscape;**

Collaborative warning between policy and analysis (intelligence);

Reommending dedicated analytic resources to **specialized tradecraft;**

Tactical warning as specific incidents, seeks to limit immediate damage;

Strategic warning as the character of threats; might require re-evaluation of strategy and assets; well in advance of incident-specific indicators;

The first phase of axial coding began after initial and focused coding was completed for most extant documents. Because all focused codes are common terms, removed from any specific work or context, all categorization was accomplished at the unclassified level. The first iteration established the initial code groupings by taking all focused codes from approximately 10 scholarly articles. After this initial set of groups was created, the axial process proceeded document by document, assigning focused codes from each new source into the existing structure, splitting or rearranging groups as necessary.

The first coding phase resulted in 227 coded entries with 169 unique codes. For repeated codes, the decision was made to focus on quality over quantity, as the number of times a code occurred was less important to determining theoretical significance than its meaning and importance in the context of the original document and overall literature. Thus, once a code was included from a source, that same code was included again only if its context was sufficiently different. This prevented common terms, such as warning, surprise, or uncertainty, from being counted several times in the same document. Limiting the number of repeat codes proved especially necessary when grouping entries from several book chapters. For example, despite the term "strategic warning" occurring hundreds of times across the set of evaluated documents, the unique code "strategic warning" was counted only five times among the 227 entries. First-level groups of codes were then labeled as categories in an iterative process during which some codes were transferred between categories to provide more coherency and other categories were relabeled. The process resulted in 28 individual first-level categories.

The final step, theoretical coding, generally followed the methods and principles established by Charmaz.[180] First-level categories were grouped into broad categories and then organized into a final, third level of theoretical concepts. The overall process of coding documents in the first research phase established 4 themes, 11 categories, and 28 subcategories.

Phase 2: Expert Consultations and Coding

While interviews and observations are the primary data-collection/generation means for an increasing majority of grounded theory studies,[181] discussions with IC personnel represent a smaller part of this study. The iterative coding process of this phase revealed that the overall project was achieving theoretical saturation, with fewer and fewer new codes being added, and eventually no changes to subcategories, categories, and themes. Thus, the determination was made after conducting 11 interviews and integrating notes from an NIU workshop on warning that the project had achieved sufficient theoretical saturation.

Interviewees[**] were drawn from the IC analytic and leadership community, spanning the defense warning community at multiple combatant commands at the line analyst and senior leadership levels and from ODNI at the line analyst and senior leader levels. A total of 11 individual discussions occurred between March and May 2023, either in person or by secure teleconference. All discussions used the same series of approved questions, although each individual session maintained the option to focus on specific questions or address other topics that came up during the session. Interview questions are provided in Appendix B. Because discussions were held at secure venues or by secure desktop video-teleconference, no recordings were allowed. All conversation notes were hand-written by the researcher and then immediately transcribed

[**] While the terms "interview" and "interviewee" may be used throughout this *Monograph,* the NIU Institutional Review Board (IRB) process determined that the types of discussions required for this project fell under the category of "expert consultation." Thus, all discussions were considered expert consultations for the purposes of human research requirements. The researcher, however, maintained a strict interview protocol of anonymity, data handling, and confidentiality to ensure strict compliance with the IRB if any discussions would need to be reclassified as interviews.

with contextual comments into the same classified Microsoft OneNote file used in phase one. Initial and focused coding employed the same procedure as previously described for phase one.

Additionally, the views of several mid-level and senior IC personnel with a distinct connection to the warning mission were integrated through notes taken at an NIU-sponsored workshop. The makeup of the workshop and its discussion prompts aligned with the same sampling population and research objectives as this *Monograph.* Approximately 25 IC personnel gathered on May 11, 2023, for a workshop, titled "Exploring the Foundations and Frontiers of Warning." Attendees represented a wide swath of IC and law enforcement agencies. Participants were divided into four cohorts and addressed six discussion prompts in two sessions. Questions presented to the workshop are provided in Appendix B. Facilitation for each group discussion was conducted by NIU personnel, with two or three note-takers per group (including the primary researcher for this *Monograph*) to ensure as complete a record of key discussion points as possible. The event was conducted within a secure facility among individuals with active security clearances to facilitate classified discussion. After the event, individual facilitators transcribed their notes, and copies were provided in support of this *Monograph.* Individual notes were copied to the same classified file notebook used for interviews, and the previous process of initial and focused coding was once again used. Coding for phase two employed the same overall methods as phase one in that duplicate codes in the same interview or discussion group were only included if they were used in a sufficiently different context.

Final Theoretical Coding and Data Processing

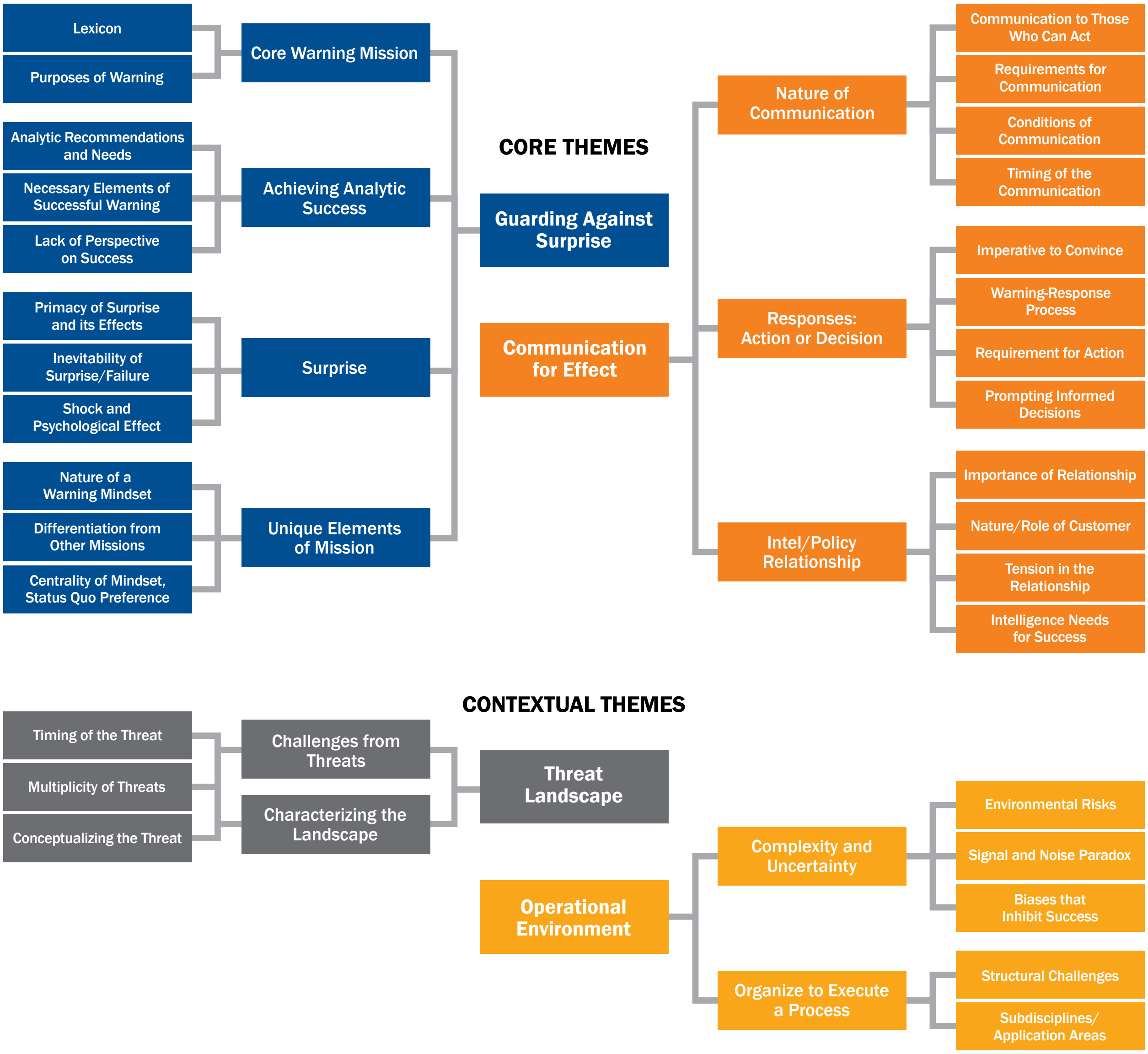
The final phase of theoretical coding and categorization was performed in an iterative fashion after conducting two to three interviews, after the NIU workshop, and with a small number of additional extant documents (included in Appendix A). Focused codes were taken from each document, interview, or group discussion and integrated into the existing theme-category-subcategory construct.

A total of 231 additional codes were added for data analysis, with 96 new unique codes identified. This relatively large influx of data had minimal impact on the overall theoretical coding, however. Despite doubling the number of codes and increasing the number of unique codes by just over half, only three new subcategories were identified, two categories were merged into one, and only one new category was added. The four core themes remained unchanged.

As each iterative addition of codes occurred, the process eventually reached a point at which no real change to the total number of unique codes or overall categorical structure occurred. This stabilization indicated that data collection had reached a point of sufficient theoretical saturation, and the research was ready to move to data analysis and reporting. (See fig. 7).

All told, the grounded theory review of warning-related documents and discussions with IC experts described in the previous section yielded 265 unique codes, listed by theme in Appendix C. From this rich field of data, the iterative process of sorting and grouping established a "map" of warning consisting of 4 core themes, 11 categories, and 31 subcategories, concluding the data collection and processing phase of research.

Figure 7. Final Map of Codes Into Themes and Categories.


Lexicon
Purposes of Warning
Core Warning Mission
Analytic Recommendations and Needs
Necessary Elements of Successful Warning
Lack of Perspective on Success
Achieving Analytic Success
Primacy of Surprise and its Effects
Inevitability of Surprise/Failure
Shock and Psychological Effect
Surprise
Nature of a Warning Mindset
Differentiation from Other Missions
Centrality of Mindset, Status Quo Preference
Unique Elements of Mission
CORE THEMES
Guarding Against Surprise
Communication for Effect
Nature of Communication
Communication to Those Who Can Act
Requirements for Communication
Conditions of Communication
Timing of the Communication
Responses: Action or Decision
Imperative to Convince
Warning-Response Process
Requirement for Action
Prompting Informed Decisions
Intel/Policy Relationship
Importance of Relationship
Nature/Role of Customer
Tension in the Relationship
Intelligence Needs for Success
CONTEXTUAL THEMES
Timing of the Threat
Multiplicity of Threats
Conceptualizing the Threat
Challenges from Threats
Characterizing the Landscape
Threat Landscape
Operational Environment
Complexity and Uncertainty
Environmental Risks
Signal and Noise Paradox
Biases that Inhibit Success
Organize to Execute a Process
Structural Challenges
Subdisciplines/ Application Areas

This page is intentionally left blank.

Grounded Theory Analysis and Findings

The four themes established from the collected data can be separated into two major themes and two contextual themes, based on the number of categories and subcategories in each. The two major themes—guarding against surprise and communicating for effect—establish the "what" and "how" of the mission. The two contextual themes—threat landscape and operational effect—establish the setting in which warning takes place.

From these core themes, a full vision of warning, grounded in data, begins to emerge. Warning guards a nation against surprise, ensuring decisionmakers and policymakers accurately understand the full landscape of threats, as well as the opportunities, they face. The act of warning requires intelligence services to explicitly communicate those threats and opportunities to achieve an effect, prompting and enabling an informed response to address, prevent, or mitigate a threat. This warning-response process occurs within the context of both the threat landscape and the broader operational environment.

The next task is to consider the elements of each theme (the categories, subcategories, and most theoretically important concepts) and establish the most theoretically significant principles of warning. These resulting principles will form the major analytic findings of this study and establish the building blocks for a foundational theory of warning.

Core Theme: Warning Guards Against Surprise

Core Theme Category Analysis: Warning Mission

The concepts and elements grouped as the core warning mission formed two subcategories: the overall purpose of warning and the lexicon used to define warning. The variety of concepts and the degree of contrast within these subcategories speak to the difficulty in understanding and defining the mission. When taken together, however, two major impressions arise. The first is the element of warning that seeks to identify and understand the full threat landscape at a broad level. This mission aligns generally with common definitions of strategic warning or dealing with emerging threats. The second is the more detailed, "tactically" oriented task of monitoring and then preventing or disrupting specific threats.

The most theoretically significant elements are the two warning *functions* (that is, understanding and tracking the full threat landscape versus understanding and tracking individual or more specific threats) rather than the most common *terms* used to describe them (that is, strategic, tactical, emerging, enduring, and so forth). Thus, although the various terms of reference in warning are important in discussing and understanding the topic, they are not critical in and of themselves. The most important implication here is that future theoretical frameworks and definitions should not be required to continue using established terms if they are not effective.

A closer look at the items comprising the purpose of warning category reveals two additional concepts with theoretical significance: the threat landscape and opportunities. The use of threat landscape in this context acknowledges that understanding the landscape is a key function of warning. The idea of opportunities emerged primarily from discussions with current IC members and more recent literature, which noted that practitioners of warning also need to better understand how to identify and communicate opportunities to deal with those threats.

Core Theme Category Analysis: Unique Elements of the Mission

If the core warning mission is to understand the overall threat landscape, as well as certain specific topics within it, then how is that different from any other characterization of intelligence collection and analysis? Doesn't every single piece of information gathered, and every assessment formed, seek to pierce the darkness of uncertainty to give decisionmakers a more accurate picture of the world, to provide updates on critical issues, and to ensure they are not surprised? Doesn't every single analyst or collector, regardless of whether they are designated as a warning analyst, have a responsibility to provide warning of threats? What then, if anything, makes warning a distinct undertaking?

The best answer from the data, and one of the most important theoretical concepts from it, is the concept of the *mindset,* because the warning mindset is essentially the distinguishing characteristic of the warning mission. The nature of the warning mindset is oriented to consider the inductive *possibilities* of the future rather than the deductive determination of the most probable or forecast outcome. The warning mindset considers a broad spectrum of possibilities, especially those that stand in contrast to the forecast future or analytic line. Thus, the warning mindset is that of a contrarian, aware that there is always a possibility that we will be wrong. Indeed, as argued by several scholars in the debate about where failure is inevitable, the warning mindset embodies the idea that we absolutely will be wrong at some point or another. The most significant terms from the data supporting this idea include *perspective of surprise, possibilities more than probabilities, envelope of possibilities,* and *contrarian.*

This contrarian, inductive viewpoint stands in contrast to the standard mode of thinking in humans. As Heuer pointed out in his seminal work, "mindsets are quick to form but resistant to change." He points out further that "mindsets are neither good nor bad; they are unavoidable."[182] The challenge for intelligence analysis is that our minds, when working in a fast mode, as they constantly are, automatically formulate narratives, as well as cause-and-effect explanations for what we see, which we then extend into what we expect to see. Even when we attempt to be more deliberate and methodical in our thinking, the autopilot mode that Kahneman labeled System 1[183] is still engaged and pushing us toward an expectation of what is the most probable outcome. Once that expectation is established, people fall prey to a variety of mental models and biases that, while amazingly accurate in the aggregate, will repeatedly fail to be correct or efficient all the time. Despite trying to be openminded or mandating the analysis of alternatives in intelligence products, once a picture of what we expect to see forms, there is a natural pull to perpetuate that image. We use terms, such as status-quo bias and confirmation bias, to describe the effect, and they stand in contrast to other key ideas in the overall data such as imagination.

The warning mindset represents a focus on countering this principle of thought, and the warning mission is best differentiated from others by its *intent and focus* on finding threats, recognizing anomalies to what we expect, incorporating red teams, and elevating minority views.

Core Theme Category Analysis: Surprise

One of the most theoretically significant concepts, and arguably the key concept within this study, is surprise. The broadest view of the warning mission is to look at the overall threat landscape and individual threats with the aim of guarding against surprise and its effects.

The core concept of surprise is connected to the terms: urgency, suddenness, something unexpected, tipping points, dramatic events, and highly compressed timelines (that is, threats that emerged or occurred more quickly than anticipated). Even with slow-moving events or threats that evolve over time, a specific point often exists when events culminate into a singular, defining incident. Michael H. describes this in his typology of intelligence surprise when discussing tectonic shifts, specifically the Arab Spring movement from 2010-12. Although demographic, economic, social, and technological forces were in motion years before, the relatively quick sequence of deposed rulers in Tunisia, Libya, and Egypt created the psychological effect of a sudden, massive, and wholly unexpected shift in global affairs. That psychological effect of surprise warrants its own separate subcategory, looking at the degree of shock that can occur. Other terms that emerged focused on whether intelligence failure and surprise are inevitable.

Core Theme Category Analysis: Achieving Analytic Success

While warning involves both the collection and analysis of information, failures of warning are generally seen as analytic in nature. The most common colloquialisms—none of which accurately capture the complicated nature of intelligence analysis—are that analysts failed to filter the signal from the noise, put the pieces together, or connect the dots. While the largest subcategory of terms dealing with analysis enumerated the various structured analytic techniques and related terminology on warning (that is, indicators or signposts, depending on the agency), the most theoretically significant elements were those identifying what is needed for successful warning. These concepts emphasized imagination, nonlinear thinking, and the ability to think bigger and incorporate a diversity of views. The manner of thinking needed for warning success leads us to the final category: the distinct elements of the warning mission.

Core Theme Summary Analysis: Warning Guards Against Surprise

Overall, this analysis paints a picture of warning as a safeguard against surprise, enabled by a mindset that explicitly and purposefully takes on the perspective of surprise. Harkening back to Levite's definition of surprise as "the sudden realization that one has been operating on the basis of an erroneous threat perception,"[184] the distinctive mission of warning is to seek out those places where our threat perception is blind or incorrect. These concepts—surprise and mindset—stand out as among the most theoretically significant elements of the data and must be integrated into any underlying framework or lexicon.

Uncovering discrepancies or inaccuracies in our understanding of the overall threat environment, however, is only part of the equation. These discrepancies or inaccuracies must then be communicated to those with the authority to act, leading to the second core theme: communication for effect.

Core Theme: Communication for Effect

Core Theme Category Analysis: Nature of the Communication

Warning definitions routinely note that warnings are communications to those who can act on them. The data emphasize both this tailored communication and the elements needed to effectively communicate a warning. The communication must be directed toward those who are able to act against the threat. Unlike warning in relation to public safety (for example, public warnings about extreme weather, terrorist threats, or medical issues), intelligence warning appears universally directed at a small set of senior decisionmakers who possess the legal, organizational, or administrative authorities to direct organizational responses—often for a specific action rather than general awareness. Key ideas highlighting this quality are bespoke communication and tailored to a specific action. Calibrating that communication to have the most impact, however, is no easy task. It requires decisions on when to warn and how to do so effectively.

The most important attribute of effective communication, judging from the data, is clarity—encompassed in codes, such as explicit warning, clarity in communication, and precise language, and the recipients must know they have been warned. Effective warnings reflect urgency, while avoiding Chicken Little hysteria. Terms connected to this concept include *convey accurately but without hype, balance urgency against over-alarming,* and *accuracy* in general.

Accuracy in warning overlaps with guidance on when to issue a warning. Timing has two major elements. The first relates to the probability or specific timeline of the threat, ensuring the warning provides enough time for a decision to be made or, as Jones advises, to not bark too early or too late. The most significant term, based on its theoretical significance and the sheer volume of use, is *cry wolf*. Providing warning earlier in a threat's evolution provides for more decision space and more opportunities to mitigate or prevent a threat. This means assessments and decisions are made under conditions of greater uncertainty with less persuasive evidence to support action. Decisionmakers may say they want to be informed about a problem as early as possible, but they also admonish against warning without a requisite level of certainty that the threat exists.[185] After all, investing in preventative action for a threat that does not occur can appear wasteful, while waiting for a satisfactory level of certainty can delay the warning beyond the point where reactions will be effective or even possible.

The second consideration on when to warn is the threat's trajectory. One option is to warn when the analytic line changes (for example, We previously assessed X, but now assess Y.). This communication potentially requires both the IC and the decisionmaker being warned to update their understanding of a threat. Warnings can also be issued when the overall trend changes, such as when a stable situation begins to deteriorate or improve. Finally, warnings can be issued after a qualitative or phase transition in "stepladder" models, such as the DWN's WATCHCON system.[186] Under this system, changes may be observed until they hit a critical mass of importance or a set decision point, or raise a specific consideration, such as the availability of future warnings.

Core Theme Category Analysis: Action vs. Decision

Warnings are provided with the explicit intent of achieving an effect. The most theoretically significant codes on the intent of warnings focused on how convincing and persuasive the warnings were (specified in the data through the idea of warnings as persuasion). Warnings are supposed to be distinct and have sufficient credibility to motivate.

Equally important are the less common references to warning as part of a larger warning-response process. The data reveal two potentially contrasting views of the intended response: 1) warning must prompt an *action*, or 2) warning must prompt a *decision*, which includes deciding not to act. Dahl's Theory of Preventative Action (taken from his seminal exploration of intelligence and surprise attack) emphasizes action, and some believe the intent to prompt an action is what differentiates warning from current intelligence or other products that are primarily intended to inform or provide context. The problem with the view that links warning to action, even if not a specific one, is that it potentially contradicts the belief that intelligence should be policy agnostic. If warnings must be so persuasive as to prompt an action, then warnings can be seen as advocating for a general or specific policy outcome. The alternative view that warning prompts a decision potentially resolves this contradiction. Here, the critical terms from the data are *decision space* (a concept especially prevalent in DoD writings and discussions), *decision advantage, decision support,* and the concept of warning as the *interaction of intelligence and decisionmaking.*[187] This raises the possibility that a decision not to act is equally viable for intelligence success. It also acknowledges that, in some situations, taking a specific action may not be politically or tactically possible.

One observation of interest in this debate is the distinct split in the origins of the data connected with action or decision. The established literature on warning, especially older documents, focused more on warning as persuasion that results in an action. In discussions with current intelligence practitioners, however, they overwhelmingly interpreted warning as prompting a decision. One potential explanation is that the literature is biased toward discussions of military attack, surprise attack, and the overriding threat of USSR military action during the Cold War. Assessing direct targets of more existential threats might warrant a more forceful view of warning. For example, Dahl focuses on military and terrorist attacks, where the metric of success is clearer—an organization either took action to prevent or disrupt an attack or it failed to act and experienced the attack. This metric is essential in Dahl's Theory of Preventative *Action* (emphasis added). Current practitioners of warning, however, discuss the topic within a broader threat landscape that includes internal instability, economic contagion, collective action phenomena, or diplomatic surprise, where policy success is more nebulous. That said, the IC is open to a criticism that it has not communicated forcefully or clearly enough if it fails to persuade a decisionmaker to act, and the threat then occurs.[188]

Under this *Monograph's* premise that warning is a social construct, the resolution to this debate is less about a correct answer than determining how the IC decides to define warning success, in keeping with its principles and mission. Any accusations arising from unheeded warnings may simply reflect the idea that there are no policy failures in national security, only intelligence failures.

Core Theme Category Analysis: Intel/Policy Relationship

That dichotomy between intelligence failure and policy success brings us to the final element of viewing warning as communicating for effect—that intelligence providers and policymakers are intertwined in a relationship that defines the warning-response process. The process cannot occur without both participants, harkening to the military adage that "intel without ops is meaningless, and ops without intel is blind." Although warning relationships are often framed as existing between the intelligence officer providing the warning and the principal decisionmaker who is making a decision, the broader connection between the intelligence and policymaking communities is equally important, especially in military organizations where relations are described as between intelligence professionals and friendly force planners, operators, capabilities, and commanders—sometimes referred to as red-blue relations.

When looking at the importance of the relationship between intelligence professionals and decisionmakers or policymakers, the most theoretically significant codes are *trust* and *receptivity.* Repeated personal interaction can build trust, but so does credibility, which cautions against repeated warning. The seminal work exploring the importance of receptivity is Dahl's comparative case study of Pearl Harbor and the Battle of Midway. Receptivity to intelligence is a critical element of Dahl's Theory of Preventative Action.[189] Studies of how trust forms between the intelligence and policy communities highlight the importance of repeated, personal interactions. For example, the impact of the relationship intelligence briefers build with their principals over time cannot be understated.[190]

The need for trust is contrasted, unfortunately, with the natural tension in the intelligence-policy relationship. In most Western nations, this tension partly arises from the view that intelligence's function is to speak truth to power. Warnings, by their nature, are often unpleasant and may divert time and resources away from preferred policy programs or proposals. Additionally, warning often represents a dissenting voice. Its intent is to prevent surprise, which implies communicating information that contradicts decisionmakers' existing understanding of the threat environment. Intelligence warnings can also conflict with the views of individuals within a decisionmaker's circle of trust, which may affect the warning relationship.

When considering how to achieve success in communicating warning, two themes emerge from the data. The first is understanding the decisionmaker's world. This includes understanding the broad dynamic described above between the intelligence and policy worlds, but also understanding the specific challenges and pressures decisionmakers face—expressed in codes such as the *opportunity costs of being wrong,* the *costs of preparation,* and *the role of [intelligence] consumers in failure*. At the specific level, whether it be a specific decisionmaker or a specific issue, successful warning requires understanding the detailed policy space (particularly from a blue-force perspective), the decisionmaker's priorities, what decisionmakers need to know, and the overall consumer process. The second theme emphasizes presenting more than just the bad news component of warning. The ideas that inform this theme include *opportunity analysis* and *solutions and not just problems.* One perspective of interest to the IC is to take on a model of warning as a joint risk-management enterprise between intelligence and policy.

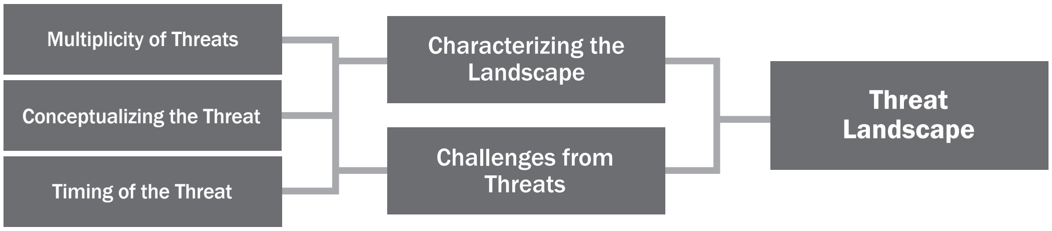
A final theoretically significant idea is that of *educated consumers.* This does not allude to consumers' often being highly educated and knowledgeable individuals in their fields or issue areas, although that must be understood as part of the overall relationship. Rather, it means that the best partners in a relationship are those educated about the intelligence process.

Core Theme Summary Analysis: Communication for Effect

Warning cannot happen unless information and analysis about a threat is communicated to a decisionmaker with the authority to act, and it can only be effective if it prompts a decision or action in time to affect that threat or its consequences. The overall theme of *communication for effect* demonstrates that the IC cannot simply focus on its half of the warning-response process. It must fully understand what makes for a persuasive or convincing communication. It also needs to recognize the supreme importance of the relationship between intelligence and policy, at both the broad and specific levels. Based on this observation, one of the most theoretically significant codes from this theme is that of *intel-policy,* a code that emphasizes the need for each domain to better understand the other. Time spent understanding and appreciating the other side of the relationship, becoming a more knowledgeable participant in the process, and strengthening personal and professional relations is time well spent in the pursuit of better national security outcomes.

It is now time to turn attention to the contextual themes, starting with the context of the threat landscape and the challenges it poses to the warning mission. (See Fig. 8).

Figure 8. Categories and Subcategories Within the Threat Landscape Theme.



Contextual Theme Analysis: The Threat Landscape

Contextual Theme Subcategory Analysis: Multiplicity of Threats

The *multiplicity of threats* faced is an important concept in two regards. First, the sheer volume of threats the IC now considers—from conventional military actions to cyber attacks, pandemic disease, state instability, space threats, foreign malign influence, terrorism, and more—is a fundamental attribute of the overall challenge. The IC will never have enough analytic or operational resources to fully explore, prepare for, or even imagine every threat.

Second, the fact that threats will always outnumber resources necessitates sorting through all the possibilities and characterizing the overall threat landscape in a way that allows us to efficiently and correctly allocate resources. The concept of *triage* emerges as one of the most important because of its prominent function. As the landscape constantly shifts with emerging—and in some cases truly emergent—threats, changing threats, and fading threats, the IC needs to constantly remap the landscape to identify those issues needing immediate attention, those that can be addressed later, and those on which we can risk inaction for the foreseeable future. This means warning is inherently dynamic. Triage impacts IC decisions on which issues to continually surveil and which to revisit only periodically, as well as operational and policy decisions. Getting this task right is an absolute necessity for successful warning. Both focusing on threats that do not warrant attention and failing to recognize the critical importance of other threats undermines national security. A major challenge is determining how to conceptualize individual threats to facilitate an accurate triage process. Stated another way, conceptualization is the means and efficient triage is the end.

Contextual Theme Subcategory Analysis: Conceptualizing the Threat

Evaluating threats and determining which need a response, requires intelligence professionals and decision-makers to mentally characterize threats in terms of their potential costs, risks, and overall nature. The most prevalent mental model found in the literature on warning and intelligence, in general, is the dominant paradigm that a threat consists of *capability and intent.* As noted in Threats: Capability and Intent (p. 27), however, valid criticisms of this traditional approach exist.

Other approaches to characterizing threats include assessments on their overall likelihood, their imminence, and their impact on national security. Characterizing threats in terms of likelihood and impact establishes a form of expected utility theory: that is, the probability of an event occurring multiplied by the costs associated with the threat occurring equals the total expected cost, assuming that more "expensive" threats might be given priority over others.

In comparison to other topics within the data collected, the idea of conceptualizing, defining, and thinking about threats appears to be one of the more underdeveloped, mirroring the gap on characterizing threats established earlier (see Major Gaps and Findings). Is it sufficient to think of a threat as a capability and intent and then assess the probability based on that? More important, how do these ways of characterizing threats relate to timing?

The field of business risk management may be instructive for future developments given the similarities between intelligence warning theory and business risk management. Business risk management emphasizes identifying and characterizing risks that represent threats to businesses, then taking steps to either prevent or mitigate the potential costs of these threats.[191] The literature on business risk management may be especially helpful in showing how to conceptualize risks through frameworks and for understanding the nuances involved in responding to different kinds of risks.

Contextual Theme Subcategory Analysis: Timing of the Threat

This brings us to the most difficult element of characterizing individual threats, forecasting a threat's timing. If warning must be timely, then it follows that an assessment *must* be made—implicitly in the mind of an analyst or explicitly in an intelligence product—of how much time we might have before a threat scenario comes to fruition. Timing plays heavily in many definitions of warning, particularly strategic warning, with references to specific time periods such as "not to exceed six months"[192] or "six months to two years,"[193] and open time periods such as "months to years" or even shorter horizons.[194]

Providing any degree of precision in assessing a threat's timing is exceptionally challenging. Warnings abound in the literature against attempting to provide specific timing and timeframes for threats. An adversary may have the capability and intent to pursue a course of action, but may prefer to pursue less costly options, maneuver for a greater advantage or time, or seek to establish sudden surprise. Some threats—a global pandemic, massive earthquake, tsunami, or industrial accident—might have a high probability of happening but not any specific starting point. Similarly, it is immensely challenging to forecast collective action threats or those arising from complexity where situations can remain "ripe" for a crisis for extended time periods.

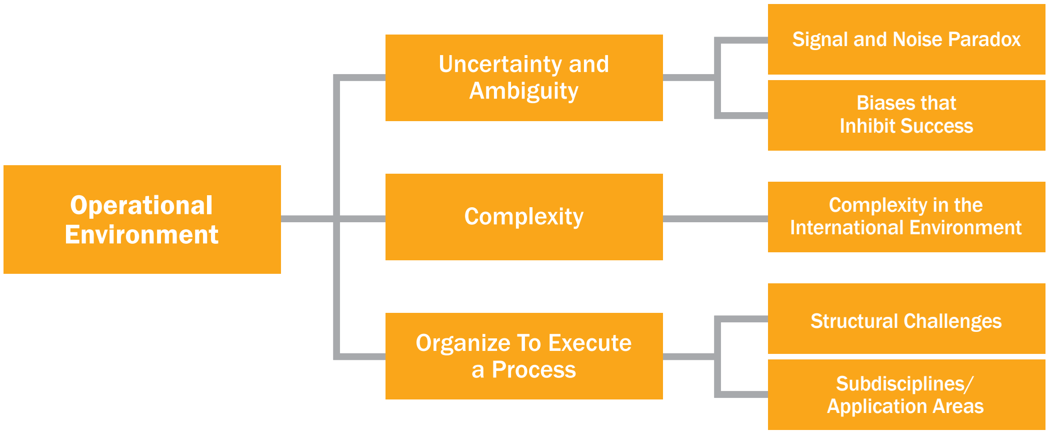
One idea that illuminates these challenges is *nonlinear versus linear threats.* Nonlinear threats are among the most challenging to forecast because they arise from complexity, where causal conditions can exist for an extended period before slight changes in inputs cause a crisis to suddenly occur. But even threats traditionally seen as linear present challenges in forecasting specific timeframes. Threats can develop so slowly that analysts either fail to detect the change or become continually accustomed to it and fail to recognize its magnitude over time—a phenomenon warning professionals call the *creep of normalcy,* akin to the boiling frog analogy. This creep can occur naturally or by adversary design. An example of a natural progression would be a volcano whose seismic activity increases so slowly over months, years, or decades that it dims our sensitivity to the signals of eruption.[195] Additionally, protests and social upheaval in a nation might increase in size or intensity over months or years, leading those who monitor them to assess that protests have been rising for years without reaching a tipping point, so why should this week's developments be any different? Jervis noted this creep of normalcy as a key finding in his postmortem on the CIA's analytic performance before the 1979 fall of the Shah of Iran.[196]

Actors can also intentionally create a creep of normalcy. Rather than alternating between building up and drawing down forces along a border, actors seeking to complicate warnings can continually increase the forces permanently stationed in an area. They can maintain high readiness levels or make frequent exercises with high readiness a normal occurrence. This creates a dilemma for defenders who must choose between making an assessment with less certainty and a weakened ability to differentiate an attack posture from a "normal" one or maintaining forces at an increased state of readiness, thereby draining financial, material, and human resources. This challenge is captured in the terms *routinization of tension* and *alert fatigue.*

Contextual Theme Summary Analysis: The Threat Landscape

In summary, the number of potential threats will always exceed the IC's or policymakers' capacity to assess and respond to them. Without nearly infinite human, material, and economic resources, advances in artificial intelligence, modeling and simulation, and quantum computing may narrow, but not close, the gap between what is needed to prepare for the threat environment and the assets available to do so. Thus, it is necessary to continually and accurately triage the elements of the ever-changing threat landscape. This mental process involves characterizing threats and their potential impact to decide what to prioritize. Perhaps the most important element of that characterization is understanding the potential timelines and timing of those threats. The concepts of the *threat landscape* and *triage* both emerge from the data as especially theoretically significant and should be integrated into any foundational theory of warning. (See Fig. 9).

Figure 9. Categories and Subcategories Within the Operational Environment Theme.


Operational Environment
Uncertainty and Ambiguity
Complexity
Organize To Execute a Process
Signal and Noise Paradox
Biases that Inhibit Success
Complexity in the International Environment
Structural Challenges
Subdisciplines/ Application Areas

Contextual Theme Analysis: The Operational Environment

Contextual Category Analysis: Uncertainty and Ambiguity

The operational environment in which threats exist is characterized by *uncertainty* and *ambiguity,* two of the most theoretically significant codes from this theme. The challenge of analysis is to gather information from this environment and then work to decrease ambiguity and uncertainty to provide the insights that allow decisionmakers to make better, more informed decisions. One way of looking at this is Roberta Wholstetter's filtering the signal from the noise.[197]

One of the more useful models for thinking about this filtering is Handel's concept that all information flows through three noise barriers: the enemy, the international environment, and self-generated noise.[198] The enemy accounts for the challenges in interpreting adversary actions and is directly related to previous discussions on adversary intent. In particular, the possibility of deception creates a paradox. Handel notes, "[because] of the great difficulties in differentiating between 'signals' and 'noise' in strategic warning, both valid and invalid information must be treated on a similar basis. In effect, all that exists is noise, not signals."[199] Handel's second noise barrier, the international environment, is encompassed in this study through the codes *complexity* (see below) and *uncertainty.* Finally, "self-generated noise" can be interpreted as the conceptual frameworks and mindsets that exist within analysts and decisionmakers.

This third barrier is the one that analysts and decisionmakers have the most control over, yet may also be the most difficult to overcome. The data emphasize the many ways analysts can fall victim to uncertainty and ambiguity: specifically, the myriad critical biases that affect warning identified by the literature and practitioners. These include well-known pathologies such as *confirmation bias, continuity bias,* and *optimism bias.* Other important codes, such as *failure to think the unthinkable*, *poverty of imagination*, *paradox of expertise,* and *unchallenged assumptions,* are noise barriers that inhibit warning, but they also echo the idea of the warning mindset established earlier. The biases themselves are not the theoretically significant data elements. The more important concept is that a warning mindset must understand and avoid these biases to counter the effects of uncertainty and ambiguity on analysis.

Contextual Category Analysis: Complexity

Along with uncertainty and ambiguity, complexity, as described in relation to anticipatory intelligence in (see p. 21), forms a third theoretically significant element of the operational environment. It is different enough from the first two to be addressed separately. Whereas uncertainty and ambiguity have always been part of the international environment, the study of complex systems shows the *complexity of the current environment is categorically different from the past.* Countering surprise from complexity will require more than just the warning mindset. The nature of complex systems requires a different analytic approach, one that may require an expanded toolkit of structured analytic techniques, including more quantitative approaches, as well as a variety of modeling and simulation approaches.

The IC's ability to counter uncertainty, ambiguity, and complexity can be enhanced by emphasizing the warning mindset. Analysts and warfighters can accomplish this by specializing in warning, training to overcome analytic bias, developing quantitative and systems analysis expertise, and employing analytic review structures/standards that emphasize the mindset. The organizational structures, training programs, and production procedures that do these tasks form the context of how the IC organizes itself to accomplish warning, the final major category within this theme.

Contextual Category Analysis: Organize To Execute

The principle of the observer effect in physics—sometimes described, mistakenly so, as the Heisenberg effect or Heisenberg's uncertainty principle—states that the very act of observing a system has an effect on the system under observation. In a similar vein, the very way we seek to organize ourselves in the IC, the way we seek to execute the broader intelligence mission, and the demands of our customers can all affect how well we execute that mission and provide warning. The most important idea here is the debate among centralized warning organizations considering all analysts as EAAWA.

This debate over manning, whether warning should be considered a separate discipline with dedicated personnel or a generic task for all analysts, is perhaps the most important and least agreed-upon debate in the field. It seeks to establish "role clarity" to identify who specifically is responsible for ensuring warning occurs. Gentry and Gordon, strictly against the notion that every analyst is or can be a warning analyst, formalized the term EAAWA in the literature. *Regardless of where one falls on the spectrum of centralized versus decentralized warning,*[††] *the choice affects how individual analysts and intelligence leaders see warning and how much emphasis it receives in daily practice.* Although it might be tempting to think that dedicated teams working with a well-formed process might be a better solution, challenges such as a *ritualized mission* or *the trappings of doctrine* demonstrate that even well-meaning efforts to adequately attend to warning can do harm. Another important concept, the *bystander effect,* can manifest when those outside a warning team assume the team will perform all warning rather than personally ensuring warning occurs. Even in an EAAWA organization, the bystander effect can occur if everyone assumes somebody else will take care of the obvious warning.

Warning can also be affected by the overall organizational structure of entities that assess geographic and functional issues. Nearly all intelligence apparatuses are divided to allow some degree of specialization, even though doing so unavoidably creates artificial *gaps and seams* in the mission. For example, consider China's increasingly global presence. Who should be responsible for working to identify threats emerging from China's interaction with nations in Africa or South America? Individuals focused on assessing China's capabilities and intent may see this as a problem for the Africa or Latin America analysts, who may see these as a "China issue" they lack the expertise to address. This gets more complicated as we add in the topics that a national security apparatus must consider military action, political instability, cyber, space, counterterrorism, counterintelligence, emerging technologies, weapons of mass destruction, transnational issues, or global pandemics. This partial list underscores the massive scale of the threat landscape. Organizational boundaries and analytic areas of responsibility are needed to operate in such a landscape. They are neither good nor bad in and of themselves, only necessary. Intelligence leaders have developed a mantra for overcoming these artificial seams and gaps: coordinate, cooperate, collaborate, or integrate (a problematic tumble of terminology that suffers many of the same issues as the debate over warning definitions). While collaboration can be effective, it must overcome yet another perennial challenge, the *tyranny of the now* or of the *urgent.*

[††] It should be noted that, while Gentry and Gordon advocate strongly against the EAAWA model, they do not advocate for an entirely separate or centralized approach, appearing to favor what they refer to as a hybrid model.

The need for decisionmakers to continually triage both their own policy preferences and the information that intelligence provides, while contending with the ever-present crisis of the day, can create a bias for current information that is more immediately actionable. The pressures on policymakers to do something about an issue as soon as possible can create an immense demand signal for shorter-term analysis. This demand for intelligence that addresses high-visibility events contrasts with the need for analysis that identifies threats for proactive rather than reactive attention. It also emphasizes speed and decisiveness over reflection and a full consideration of the uncertainty around an issue.

Additionally, much of the IC mirrors the "publish or perish" mentality of academia, making the number of intelligence products produced the most important metric for evaluation, promotion, and compensation. This, too, creates a bias toward an immediate focus and moving on once an assessment is made. One NIU study raised the possibility that even when analysts worked to provide warning of potential threats and establish indicators for them, their efforts did not receive sufficient follow up,[200] possibly because of the pressure to move on to the next topic. This reality stands in stark contrast to Grabo's central assertion that warning is an exhaustive research process that requires analysts to consistently evaluate new information in the context of past developments and in a wider time horizon both forward and backward.

Contextual Theme Summary Analysis: The Threat Landscape

In summary, warning occurs within the context of both the natural global environment and the artificial constructs of institutional structure and organization. The most theoretically important elements of this context, from the notions of uncertainty and analytic bias to the tyranny of the now, can be especially frustrating in that arguably nothing can be done to eliminate them. We can no more erase ambiguity from information than we can eliminate bias from our thinking or remain consistently conscious of all the elements that comprise our mindsets. These contextual challenges are a fact. What individuals and organizations have control over is their cognizance of the issues and the application of continued effort to counteract them.

Final Results: *The Fundamental Principles of Warning*

Seven fundamental principles of warning capture the most theoretically significant elements from the data collected and the preceding analysis. These principles provide an answer to both the primary and secondary research questions established at the outset of this study. More important, they form the foundational building blocks on which a theory of warning and associated lexicon may be built.

1. **Warning Counteracts and Mitigates Surprise**: The notion of surprise, including the traumatic psychological effects it can produce, is one of the most theoretically significant terms in warning. By focusing on reducing surprise, warning enables decisionmakers to prevent threats or, when prevention is not possible, ensures they are not wholly unprepared, having failed to take preventative or preparatory measures they otherwise would have.

2. **Warning Requires a Distinct Mindset**: Countering surprise means understanding the context of the global environment and the threat landscape within that environment. It also means recognizing that there are, at any given moment, a multitude of possible futures and that unforeseen or unlikely futures will inevitably occur over time. If surprise is indeed inevitable, then a warning mindset can at the very least ensure a mode of thinking that appreciates multiple futures and thus reduces the overall chances of a catastrophic surprise. This mindset retains cognizance of the impact of uncertainty, ambiguity, and complexity on both the threats and how we perceive them.
3. **Warning Must Be Timely and Account for Time**: Although specific timeframes are problematic, the notion that warning must be timely is critical to any theory and lexicon. Warning must provide decisionmakers the opportunity and time to orient and decide whether and how to act.
4. **The Complete Nature of the Warning Mission**: Warning occurs across a broad spectrum and includes multiple implied tasks. The theoretically important elements are the implied missions, which include identifying emerging threats, exploring future scenarios, triaging threats through characterization and prioritization, and detecting when identified issues begin to transition to crises.
5. **Warning Is an Explicit Communication**: Collection and analysis are elements of successful warning, but warning cannot occur unless that information and analysis are explicitly communicated to decisionmakers with the authority or capability to affect action.
6. **Warning Must Persuade Decisionmakers**: Warning's distinguishing purpose is not to simply provide information or situational awareness, but rather to persuade, to convince, or to *make it stick.*[201] Successful warning should prompt a distinct decision point, and while many might argue that the decision should result in a subsequent action, the importance placed on maintaining a policy agnostic, objective posture by current practitioners leads this research to propose that a distinct decision point is the minimum condition for warning success.
7. **The Importance of the Intelligence-Policy Relationship**: Warning is simply the first element of the overall warning-response process, and as such represents the most important intersection between the intelligence and decisionmaking communities. This intersection forms the basis of a relationship, both at the general level and most especially at the level of individual exchange where participants build trust and receptivity. Both the intelligence provider and consumer must be educated participants, understanding the context and constraints of the other.

(Re)-Defining Warning

The IC has long recognized the need for a commonly accepted definition of warning to improve performance but establishing one has been challenging. A lexicon that is inconsistent, unclear, or contested can affect more than just intelligence production and organization. It can also affect how decisionmakers perceive and evaluate warnings.[202] For example, intelligence scholars have noted issues caused by multiple interpretations of the term "strategic,"[203] which when applied to warning can affect interpretations of what a "strategic warning issue" is, what "strategic warning" entails, and who is responsible for it. Warning is more likely to be effective when there is a more universal understanding, by the IC and decisionmakers, of what it entails. In pursuit of this goal, an effective definition for warning, or set of definitions that form a core lexicon, should seek to include the fundamental principles identified previously. Many definitions of warning proposed during the past several decades have incorporated some of these elements, particularly communication and timeliness (see pp. 23-25, "Defining Warning"), but no *singular* definition or series of definitions has effectively done so yet.

Critiquing Historical and Contemporary Definitions

The best existing off-the-shelf definition of warning, based on the criteria of addressing the most foundational principles, is provided by Davis. He proposed that "warning analysis seeks to prevent or limit damage to US national security interests via communication of timely, convincing, and decision-enhancing assessments that assist policy officials to effect defensive and preemptive measures against future threats and to take action to defend against imminent threats." Davis emphasized communication, timeliness, and persuasion, and he addressed the dual missions of identifying future threats and monitoring established threats (or imminent as he specifically stated). He did not sufficiently integrate the themes of surprise or mindset, however.

DoD also provided an extensive series of terms over time that address some, but not all necessary principles. DoD can be seen as a gold standard for lexicon and definitions given its extensive library of official doctrine, directives, and instructions, its detailed system for establishing and updating terms, and its Dictionary of Military and Associated Terms.[‡‡] The DoD definition of warning

[‡‡] DoD terminology operates based on Chairman of the Joint Chiefs of Staff Instruction 5705.01. The DoD Dictionary of Military and Associated Terms, previously published as JP 1-02, transitioned to be more flexible and exists primarily online at https://jdeis.js.mil/jdeis/index.jsp?pindex=4, which requires a DoD Common Access Card login. This dictionary

intelligence[§§] at the time of this writing is "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests."[204] Meanwhile, DoD Directive 3115.16, the policy document establishing the DWN, defines warning as "a communication and acknowledgment of dangers implicit in a wide spectrum of activities by potential opponents ranging from routine defense measures to substantive increases in readiness and force preparedness and to acts of terrorism or political, economic, or military provocation."[205] Finally, the 2017 *DWN Handbook* defines warning as "a distinct communication to a decisionmaker about threats against US and allied security, military, political, information, or economic interests. The message should be given in sufficient time to provide the decisionmaker opportunities to avoid or mitigate the impact of the threat."[206] None of these definitions are wrong, incorrect, or broken, but they do not capture the full scope of warning and its most theoretically significant concepts. In particular, the joint doctrine document provided a modest definition of warning and continually reduced its warning lexicon over the years (most likely to avoid a confusing mix of terms that had grown over time, including "indications and warning," among others).

Granted, a singular definition that captures all principles of warning is untenable, if not impossible, without becoming a burdensome wall of text that confuses the mission more than clarifies it. As soon as multiple terms are needed, we cross from the need for a definition to the need for a lexicon. As noted, the dominant means of expanding the vocabulary of warning over time has been to delineate between strategic and tactical warning. This distinction can be problematic, however. First, there has never been agreement on what the distinction is between strategic and tactical warning, and many of the distinctions that have been used leave gaps in the mission. Davis's approach was to set up a broad, specific distinction between the two disciplines, but as noted previously, this is a unique approach compared with how others view the distinction.

Most Cold War definitions of strategic and tactical warning dismissed tactical warning as a military issue and considered strategic warning to encompass everything up to the initiation of an attack or key event. Over time, DoD has shifted this view to see strategic, operational, and tactical warning as all occurring before an attack, thus creating a distinction that mixes scope with timelines as demonstrated by the following trio of definitions and notes from the 2017 *DWN Handbook.*[207] (see Table 1)

For many reasons, strategic and tactical are best used as relative terms to provide direction in scoping analysis (that is, "we need to think more strategically" or "we need to focus on more tactical decisions"), rather than absolute categories of time or threats. The terms can lead to fruitless debates over what counts as a strategic threat (for example, whether the 9/11 attacks or the Colonial Pipeline attack should be considered strategic threats.)[208, 209, 210]

collates definitions from the full library of DoD doctrine, and most definitions dealing with intelligence, including warning intelligence and threat warning, are cited from JP 2-0. This *Monograph* adopted the convention of citing the original doctrinal source and not the dictionary itself.

[§§] A definition for warning as a standalone word is not included. JP 2-0 only provides definitions for "warning intelligence" and "threat warning."

Table 1: DWN Definitions of Strategic, Operational, and Tactical Warning.

Strategic Warning	Operational Warning	Tactical Warning
Definition: A warning communicated to decisionmakers of developments or events that create the conditions for risk of conflict or other events detrimental to the security of other interests of the nation and allied partners.	**Definition:** A warning communicated to decisionmakers of developing situations or ongoing events that significantly increase the potential risk to the security or other interests of the nation and allied partners.	**Definition:** A near-term warning communicated to decisionmakers of an imminent or ongoing attack, or other potentially hostile activity. Tactical warning is intended to alert decisionmakers who must respond with little or no time to take precautions or counteractions.
Example: Increased political and economic tension between two states. Situation developing that could lead to unrest, military action, etc.	**Example:** The forward-positioning of assets that could be used in a military campaign. Conflict/crisis not inevitable, but actors are preparing to engage in conflict, unrest, etc.	**Example:** A cross-border military incursion into an enemy state. Conflict/crisis is imminent or under way.
Timeline Notes: Months to years before the threat materializes; sufficient time for decisionmakers to mitigate the risk.	**Timeline Notes:** Typically, days to weeks before the threat materializes; time for decisionmakers to mitigate risk exists but is limited.	**Timelines Notes:** Typically, hours (or less) until risk materializes; little to no time for decisionmakers to mitigate risk but conveyed in enough time so decisionmakers can avoid surprise.

Source: Author's table based on DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

More important, differentiating between strategic and tactical warning has the potential to create unnecessary administrative and territorial arguments. Organizations can use these definitions and any associated timelines to lay claim to mission areas or to avoid inconvenient tasks. If we define strategic warning as involving issues six months to two years from occurring, then it becomes possible to dismiss issues not assessed to fall within that timeframe. Differentiating between strategic and tactical warning also establishes an artificial seam or gap between missions as threats transition from long-term concerns to more immediate crises. In particular, the term strategic can be used to imply importance or hierarchal dominance. This is especially pronounced when strategic warning is defined as providing warning to a nation's most senior leadership,[211, 212] or when it may be considered more important or useful than other types of warning.[213] A counterargument for using strategic warning as a term is that it lends gravitas or importance to the mission, which can be a motivating point when working to encourage analysts or organizations to dedicate time and resources to the task. But as long as strategic warning can be contrasted to tactical warning, the possibility exists for anything nonstrategic to be viewed as less important when, in reality, it is essential for warning to occur on an ongoing basis at multiple levels of government up until the moment of an event.

The other major problem with existing definitions of warning is a tendency to specify timeframes. Although time and timing are vital to developing a full understanding of warning, a formal lexicon should not include specific timeframes (such as six months to two years),[214] generalized timeframes (such as months to years), [215] or vague terms (such as "imminent"). Within the warning mission, time and timing are highly relative both in how individual problems play out and in what decisionmakers consider to be timely warning. Warning of and responding to a military attack may occur over a period of months, while warning about emerging technologies or demographic trends may involve decisions on research, investment, and budgeting that must be made and executed years in advance. This problem has become more pronounced as the breadth of national security threats has expanded to include cyber, disruptive technologies, malign influence, pandemics, and proliferation—which vary significantly in how quickly they mature and, therefore, the lead time needed for warning. Additionally, some threat responses might be made by individuals with delegated responsibilities, while others may require time to gain consensus or negotiate. Rather than include specified timeframes in definitions or frameworks, practitioners of warning would be better served by exploring and understanding how time relates to specific threat scenarios or classes of threats, such as military attacks versus political instability, cyber attacks, or proliferation. At a minimum, knowing what constitutes timely warning requires understanding how quickly the threat might develop and what the decision points are for responding policymakers.

When considered in its entirety, the IC has a responsibility to provide warning along the entire spectrum of threats, in both scope and time, to decisionmakers across the full spectrum of government and military functions. This means providing strategic warning to operational or tactical planning teams across the government, as well as providing tactical warning to national decisionmakers who need to make time-critical decisions.

Proposing a New Core Lexicon of Warning

No single definition of warning is likely to ever be sufficient when dealing with national security, so three core lexicon terms are proposed here: the definitions of warning as a mission, warning as a communication, and warning as a mindset.

Warning as a Mission

***Mission:** Warning is the identification, characterization, monitoring, and persuasive communication of threats against national interests with sufficient time to enable policy, planning, resource allocation, or operational responses to prevent or minimize the incidence and effects of surprise.*

Redefining warning as a mission incorporates the full spectrum of implied warning subtasks (identifying, characterizing, and monitoring threats) into a single definition that covers both the emerging and enduring nature of threats across all timelines. In doing so, it abandons the previously dominant strategic-tactical paradigm. This definition also seeks to enumerate the variety of actions that can be taken in response to a warning and charges that the warning be timely to enable those actions. Some responses may be taken unilaterally, immediately, and with available assets, resources, and plans. Others may require building consensus to initiate planning and allocate resources, or develop a new project, plan, or capability—all of which may involve time-consuming processes.

Additionally, this definition of warning as a mission specifically incorporates the objective of reducing surprise. Although this might appear to be a trivial inclusion, easily omitted with no impact to the definition, it is one of the most important elements that distinguish warning from other intelligence functions or products. The imperative to reduce surprise reinforces two ideas. First, it reminds us that the threat landscape is always changing. Surprise can occur when we are unaware of emerging—and emergent—threats, or when benign issues turn malignant. This includes changes to the international threat environment that deviate from our analytic lines. Second, it reminds us that our understanding or analysis of the world may be fundamentally incorrect, requiring us to continually reevaluate our assumptions, challenge analytic lines, and explore alternative scenarios or interpretations. These ideas allude to the theme of the warning mindset. This definition also specifically establishes the mandate for persuasive communication. Fully understanding what constitutes successful and persuasive communication, however, requires a more detailed exploration and definition.

Warning as a Communication

***Communication:** A warning is an explicit communication about an observed or potentially adverse change in the threat environment and its associated risk to national interests, so as to persuade decisionmakers or their principal advisers of the nature of the threat and to prompt an informed decision.*

Defining warning as a communication emphasizes that the action must be explicit and directed toward a decisionmaker to enable a response. The use of the words *explicit* and *targeted* is intentional. An *explicit* warning is one in which the person being warned understands that they are being warned and the warning is coming directly from a specific member or element of the IC. This does not require new intelligence product lines or tools, but to be successful, warning cannot rely on the hope that a decisionmaker "gets the message" or that a product might serve "as a warning." Unfortunately, this is arguably the way many warnings are communicated, indirectly using slides or routine production. In these cases, an analyst or office hopes that a principal decisionmaker recognizes the warning or that a briefer specifically highlights the message for them. Successful explicit communications should incorporate all four core elements of a communication process: the sender, the message, the receiver, and feedback. This idea of feedback implies a discussion or interaction to ensure the warning element of the IC understands whether their warning has prompted a decision. It further implies an interpersonal relationship between members of the intelligence and policy communities, however brief or informal.

Targeted communications must be directed, possibly through an adviser or intermediary, at the specific individual or office with the responsibility and authority to take relevant action. Finally, this definition of warning as a communication specifically notes a change in the threat environment, implying the decisionmaker's threat perception must also adapt, and it confronts the challenge inherent in updating those perceptions by noting that the communication must persuade or otherwise convince.

It is important to emphasize here that this definition should in no way be interpreted as stating that warnings must always be point-to-point communications and cannot be broadcast through more widely disseminated products. This definition represents an ideal state, in which the messenger focuses on a distinctly defined actor or actors, understands the broader context of the decisionmaker and the available options, and communicates in a way that successfully prompts a distinct decision point. Furthermore, even if a warning is expressly intended for a single decisionmaker or small group with the broadest authority to act, it is still possible for decisionmakers and groups at multiple levels to understand the warning and make their own subordinate decisions. When a national leader receives warnings about a potential crisis, commanders at subordinate and supporting levels, who might be called on to react, can make decisions to begin their own preparations or training, improving the efficiency and effectiveness of a future decision.

In sum, by including the option of warning a principal adviser, this definition recognizes the importance of relationships and that the most effective warnings may ultimately need to be delivered by another, more trusted interlocutor. Bad news may be more readily received, or at least not so easily dismissed, if delivered by a trusted friend who has a better relationship with the principal decisionmaker, is part of that decisionmaker's inner circle, or can speak in familiar terms with the decisionmaker.[216]

Warning as a Mindset

***Mindset:** The Warning Mindset is an approach to thinking about threats, by both intelligence professionals and decisionmakers, in terms of what is possible rather than simply what is probable and adheres to four fundamental tenets: the presumption of surprise, the expectation of change, the acceptance of uncertainty, and the recognition that individuals and organizations will sometimes be wrong in their understanding of the threat landscape.*

Finally, the importance of having an open, imaginative mindset is potentially a requirement for success and the most defining or distinct element of warning. Most intelligence analysis units focus on providing decision advantage to their principals and reducing uncertainty by looking to acquire information and forecast the most likely outcomes. An individual or team that wants to provide the best possible warning, however, needs the capacity to remove themselves from their normal way of thinking from time to time and explore the possibilities that exist in their issue area. This effort needs to be intentional and not just a side practice of providing passing considerations for the sake of checking a box in a tradecraft assessment (for example, "we considered the possibility that we may be incorrect in our analysis, but because we are probably correct it is unlikely that we are incorrect") or providing the traditional worst-case scenario along with the most likely scenario. Worst-case scenarios do happen, and organizations cannot ignore them, but a range of plausible outcomes typically lies between the most likely and worst-case ones—and they warrant attention as well. The core element of this mindset is recognizing that a world of potential futures exists, which can be accomplished by considering what is possible over what is probable.

The four tenets of the warning mindset are drawn from the literature on warning and intelligence analysis. First, the "presumption of surprise" is listed to reinforce once again the core theoretic significance of surprise. Studying, understanding, and learning from surprises is perhaps one of the best ways to improve warning performance. While this can include traditional intelligence success and failure case studies, it also means exploring the nature of surprises more deeply through work such as Michael H.'s development of a typology of surprise.[217] The presumption of surprise also establishes a need to embrace nonlinear thinking and recognize the possibility for nonlinear events such as tipping points or rapid escalations.

Next, the "expectation of change" emphasizes elements of the literature that see warning as change detection, anomaly detection, and recognition of discontinuities or deviations from the baseline (all arguably synonyms of the same core task). When changes occur without our knowledge, our understanding of the threat environment becomes less accurate. The expectation of change over time also implies that analysts and decisionmakers will periodically need to go back and ensure previous assessments, assumptions, plans, or policies are still accurate.

The acceptance of uncertainty integrates a key element of the operational environment and serves as its own warning of sorts against a critical error that many intelligence personnel and decisionmakers can make—the desire to wait until there is more information and more certainty. Analysts embracing a warning mindset will be more willing to provide warnings with less certain information, working to accurately frame the risk involved. Decisionmakers embracing a warning mindset will recognize that waiting for "unambiguous warning" risks losing necessary time to react and that effective decisions must manage a degree of risk. There are risks for both the warner and the decisionmaker when it comes to acting under conditions of uncertainty, but the risk is not necessarily shared equally. As Clarke and Eddy noted, it is not only the technical expert, the warner, who will be ridiculed and professionally damaged if the disaster does not come. It is, perhaps even more so, the leader who was duped into believing the warner."[218]

Finally, the recognition that one will periodically be wrong in their understanding of the threat landscape looks to caution both intelligence professionals and decisionmakers against hubris, as well as from seizing and freezing.[219] This includes cautioning against analysts who have amassed years of experience and feel supremely confident in their understanding of and expertise in their subject area (captured in data as the paradox of expertise). The recognition that we may be wrong is also an acknowledgement of the role that chance plays in making both assessments and decisions. Even with the best possible information and analysis and near certainty, we may still make the wrong call—if for no other reason than luck. Philip Tetlock describes the role chance can play in addressing a question about violence in the East China Sea as part of his Good Judgment Project, which was answered by a confrontation days before closing in a "last-last minute event that no one, this side of God, could have foreseen."[220] Finally, the recognition that we may be wrong requires us to acknowledge the fact that we are operating in a world of complexity and uncertainty.

It is not just its own warning against hubris, but a consolation when we take the risk of trying to warn and act as early as possible. It is entirely possible to be wrong, but for the right reasons.

The Foundations for a Framework

These three definitions, warning as a mission, communication, and mindset, provide the foundation for a full framework of warning, and they address most of the theoretically significant themes. Specifically, these definitions sufficiently address surprise, the distinct mindset of warning, the full spectrum of tasks involved in warning, and the idea that warning is an explicit communication. The next step in the theoretical process is to build on this foundation by looking at warning's relation to time and timeliness with a more thorough consideration of threats and characterizing threats.

Exploring Threats and (Re)-Modeling Warning

Threats and the Threat Landscape

Despite the importance of threat as a central concept in warning, the notion of what a threat is receives surprisingly little consideration. This gap is not exclusive to intelligence studies. Peter Trubowitz and Kohei Watanabe's exploration of geopolitical threat noted that "as essential as threat is to the study of world politics, scholars do not agree on how to identify and measure threats."[221] With all due deference to US Supreme Court decisions, a threat may not currently be something most people can intelligibly define, but they know one when they see it. As noted previously, the dominant view of threats within the warning literature, as well as that of some risk-management approaches, is that a threat is the combination of capability and intent. This framework is adequate for considering some threats, but it fails as a definition when a discernable central intent is not part of the equation, such as with complex systems, collective action problems, or naturally occurring threats such as pandemics. As scholars observed, it is possible for complex systems to exhibit behaviors that are not the sum of their parts or that run counter to the intent of many of the actors in that system.[222, 223] Thus, capability plus intent is insufficient for a full theory of warning.

Developing a sufficient theory or framework could draw on the literature of risk management, and lessons from both public and private risk management should be an important arena of further research for warning. For the purposes of this *Monograph,* however, the beginnings of a threat theory should be drawn from the literature and data from which the foundational principles of warning emerge.

With the exception of historical case studies, the threats discussed across the literature and by practitioners—military attacks, social unrest, cyber attacks, and so forth—are abstract conceptualizations of possible scenarios. They are abstract because they have not yet occurred in the physical world, and, in the case of historical case studies, they were abstractions before they occurred. Some warning practitioners refer to the moment when a threat transitions from abstract future scenario to historical fact as the terminal point or end state. This terminal point can be a clearly delineated moment in time, such as when troops launch the opening salvo in an attack, or it can be more ambiguous and subjective, such as determining the moment when a government loses control or when a financial collapse occurs. Threats, as described in the literature, are also negative scenarios, which is a matter of perspective. A potential future may be negative for one actor, but positive for another. For example, social instability in one nation may be considered a threat for a neighbor facing spillover or refugee flows, but an opportunity for a rival state.

From these core considerations, the definition of a threat for the remainder of this *Monograph* shall be as follows:

*A **threat** is an abstract conceptualization of a future temporal event that can occur in the physical world[¶¶] and imposes undesired costs from the viewpoint of an actor.*

A threat can be specified in any level of detail through ideas, titles, and scenarios along a spectrum that runs from broad to specific. For example, at the broadest level, a threat could be described as one country attacking another. At more detailed levels of specification, however, specific scenarios might lay out an overall expected timeline of the attack, the means of attack, and the overall strategic and tactical objectives (for example, a land attack intended to capture a small amount of territory using mobile, lightly armed infantry supported by artillery). At the most detailed, specified levels, an entire geopolitical "road to war" scenario can be created along with expected tables of organization and equipment for both the attacker and defender, which can be used to explore the threat using wargames or computer simulation.

Having defined a threat, it is now possible to consider the idea of the threat landscape. The *full* threat landscape is an infinite set of both imagined and unimagined threats (that is, those we are aware of as well as the universe of black swan events we have dismissed as impossible or have simply not conceived of yet). This landscape does not just consist of the set of different threats, but also the different ways in which they can manifest in terms of time or intensity. Looking back to our example of a military conflict between two states, the idea of a conflict can be broken down into attacks at all different types of intensities but, more important, at any specific time, such as an attack that occurs tomorrow or one that occurs a year from now. Of course, it is impossible to deal with an infinite set of threats, which is why most uses of the term probably refer to what this *Monograph* defines as the *known* threat landscape.

The known threat landscape is a finite set of those threats that are recognized by an organization or individual at any given point.[***] Some may be highly specified, while others may only be broad abstractions (for example, the decline of democracy[†††]). The known threat landscape is defined here as a finite set for two reasons. First, everyone has a limited imagination or conceptualization of the world, one provided by their underlying mindsets, heuristics, and mental frames. This limited capability puts a finite cap on the number of scenarios available for consideration at any one time. Any group, such as an analytic team or decisionmaking body, may

[¶¶] This definition includes cyber attacks because all data are manifest in the physical world in the magnetic orientations of physical hard drives, servers, and other data storage systems. Programs and codes also exist in data files and thus exist on the same variety of physical systems.

[***] The differentiation between the infinite and finite sets of the full and known landscapes, respectively, and their consideration as mathematical sets, is not necessarily important for most practical discussions or applications. As the foundation of a full, positive theory, however, the distinction is relevant for academic, theoretic, or even philosophical exploration which can, in turn, benefit the world of practical application.

[†††] The decline of democracy is an excellent example of a future development that might be seen as costly for some actors but as a positive development for others.

combine these individual sets, but the collective result is still a finite set. Second, and even more important to developing a threat theory for warning, is the way our minds simplify the world around us by grouping like ideas into finite subsets. The full threat landscape might include the possibility of an attack at every possible moment in time, but this *Monograph* proposes that the known threat landscape in our minds sort infinite possibilities into finite groups as we perform the critical mental task of characterizing threats.[‡‡‡]

Characterizing Threats

While capability and intent are important inputs into how we characterize threats, they are not the main metrics or measures of a threat. Keith Clark, in considering the timing of warnings, provides the best framework for how we characterize threats. His framework includes three elements. The first is probability (how likely an event is to occur), which is often combined with the second idea of imminence (how soon an event might occur). When considering the threat of an attack tomorrow as opposed to one a year from now, each scenario will have its own distinct probability. One will have the most likely imminence—an attack, for example, might be unlikely next week because of incomplete preparations, but much more likely in six months. Capability and intent may be the driving factors in assessing the likelihood of an event at different degrees of imminence, but the final characterization comes down to assessing how far in time we are from a possible threat. This is the *proximity in time* of the threat, the term of reference for this idea going forward. It is worth noting that surprise can occur when our perception of a threat's proximity is incorrect.

The third element in Clark's list forms the other major factor for characterizing threats, importance. The importance of a threat, as described by Clark, depends on individual viewpoints. Thus, he says that "the question of importance probably refers less to whether to warn than whom to warn and how." For this monograph, importance equates to the potential costs for national security. More important threats incur greater expected costs.

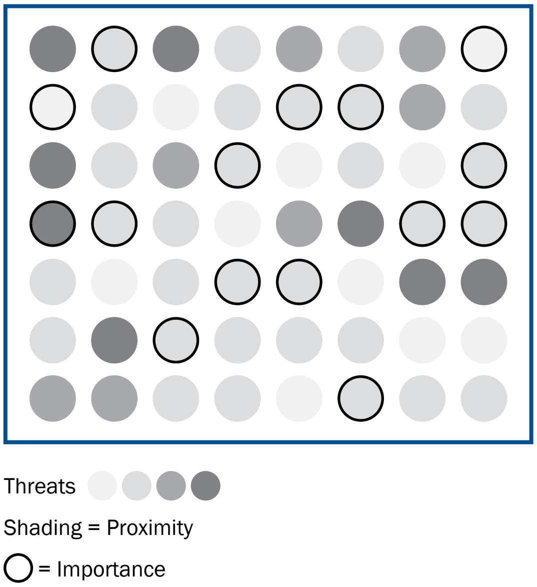
Combining imminence with the cost provides the overall level of concern about a threat. Organizations warn based on changes to their level of concern or, more important, the level of concern which a decisionmaker is likely to have. These warnings can occur when the proximity of a threat is increasing, when the costs of the threat are increasing, or when we update prior assessments about the threat's proximity or importance. These warnings seek to persuade decisionmakers to update their understanding of imminence or importance, prompting decisions on whether and how to react.

Modeling the Threat Landscape

Because the known threat landscape is the set of those threats an organization recognizes, it can be easily illustrated for explanatory purposes. In the image below, the threat landscape is modeled as a set of dots, with the shading representing the proximity of the threat (darker is closer) and a border representing an issue of importance to the supported decisionmakers. (See Fig. 10.)

[‡‡‡] This proposal is made as a fundamental assumption for this *Monograph's* purposes and could be refuted by research in cognitive science as part of a broader exploration of threat theory.

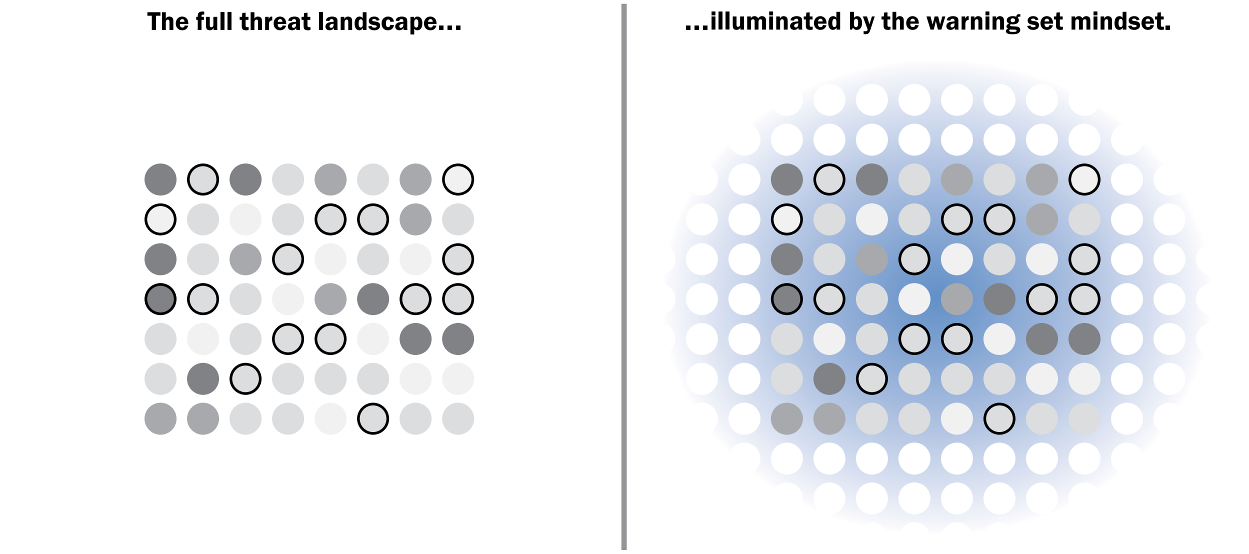
Figure 10. The Known Threat Landscape.



The known threat landscape has a distinct border around it because it is finite. An organization only knows what it knows or what it sees. The first key task for warning is recognizing and remembering that the full landscape is infinite and thus there is a need to seek out and identify other relevant threats. Sometimes they will become readily apparent over time. By looking for weak signals or adopting a warning mindset, however, individuals can change the metaphorical filter on their lens of the world to become more aware of the full threat landscape:

The second key task for warning is to recognize that both the full and known threat landscapes are constantly changing. New threats emerge, some threats disappear, a threat's proximity will change, and the importance of each threat will change, as well. Part of the task of monitoring threats presented in the definition of warning as a mission is to understand how the threat landscape changes over time and when decisions are needed to adapt postures, plans, or priorities. (See Fig 11.) There will always be more threats than the analytic or operational resources to deal with them. Thus, monitoring threats requires a constant triage process to determine at a given time which problems are most important and warrant increased attention, contingency plans, or immediate action.

Figure 11. The Warning Mindset Illuminates the Full Threat Landscape.

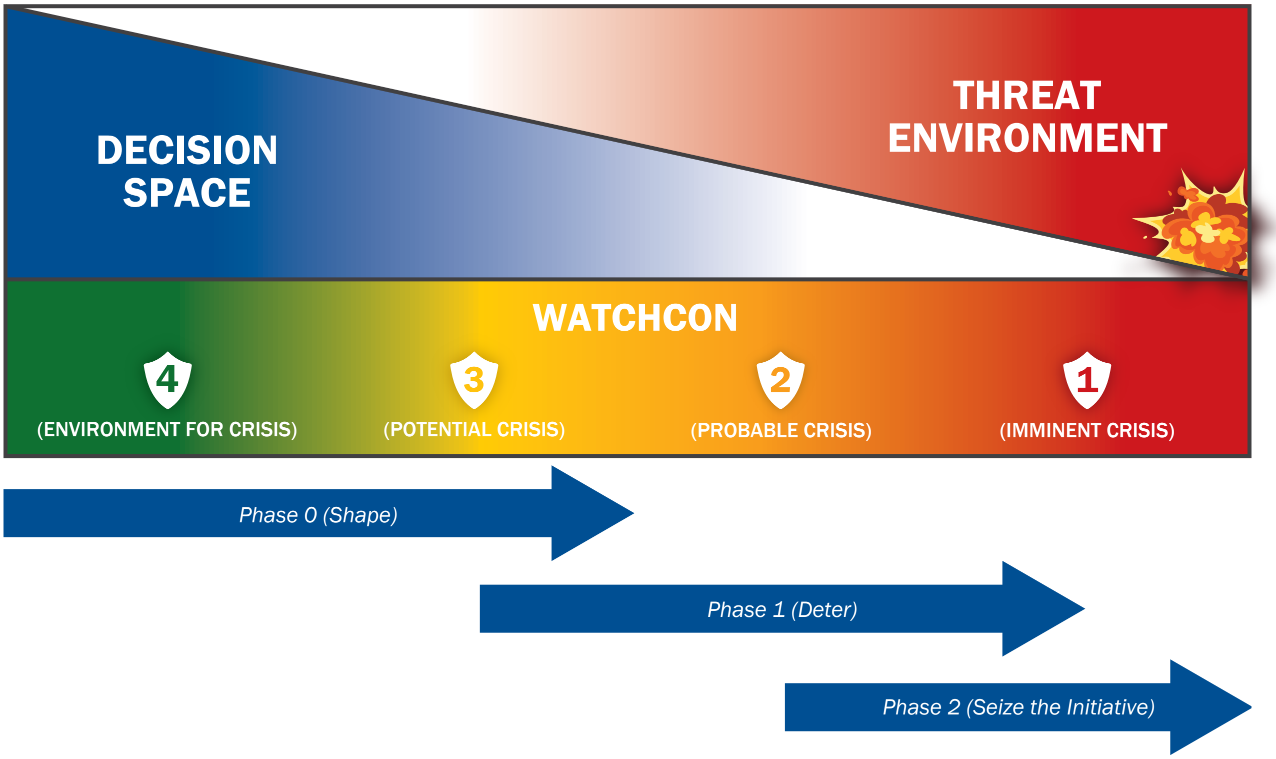

The full threat landscape...
...illuminated by the warning set mindset.

Within the specific doctrine of the DWN, problems considered to be the most important for decisionmakers, specifically combatant commanders, are elevated to the status of an enduring warning problem as part of strategic warning. Davis's view of warning probably would label this process tactical warning or incident warning. In either case, the intelligence apparatus focuses on warning about a focused set of specified, individual threats. As described above, the assessment of how much time we might have before a threat occurs is the threat's *proximity in time.* Equally important, however, is the threat's possible *proximity over time.*

Modeling Individual Threats: Proximity in Time Versus Proximity Over Time

An earlier critique of warning definitions that specify distinct timeframes was that each threat is unique in how it might evolve over time. Threats can take a different series of paths through time, with some requiring long lead times while others can develop and occur more quickly. Thus, while the proximity of a threat is an essential intelligence assessment, analysts and decisionmakers also need to understand how that proximity has varied in the past and how it might progress in the future. No current model of warning effectively does this, but the DWN model comes closest and is arguably the best theoretical model of warning. Within the DWN model of threat progression and decision space (see Fig. 12), time might not be specifically labeled, but it is implied as a threat progresses from a lower-level concern during Phase 0 to greater levels of concern

Figure 12. The DWN Decision Space Model.



Source: Adapted from DOD Inspector General (IG); DODIG-2020-055; January 30, 2020; "(U) Evaluation of US European Command's Warning Intelligence Capabilities," (Redacted); Classification of extracted material is U; Overall classification is U. https://www.oversight.gov/report/dod/evaluation-us-european-commands-warning-intelligence-capabilities.

during Phases 1 and 2. Within the DWN warning methodology, the WATCHCON communicates the level of concern, which varies from 4 to 1.[224]

The main problem with the implicit incorporation of time in this model is that it shows or assumes a linear progression. Although the relationship between decision space and levels of concern (as demonstrated by the various WATCHCON's color shading) may be linear in some cases, that might not hold true for all threat types. Recall that this study identifies nonlinear threats and nonlinear thinking as important terms (see Appendix C). Thus, a sufficient model of warning needs to consider, and indeed emphasize, nonlinear thinking.

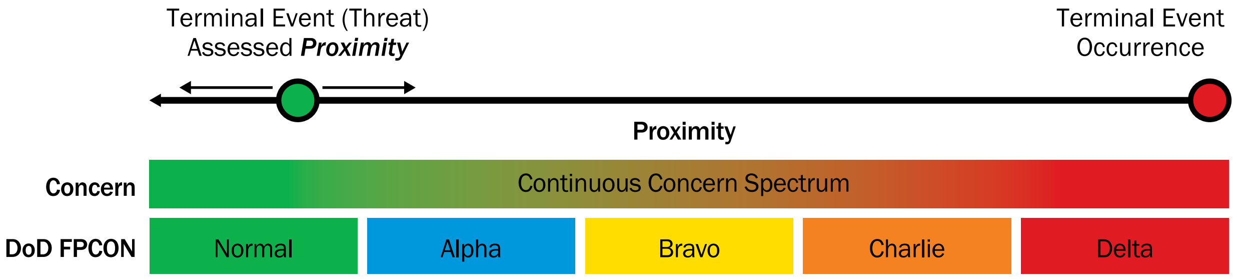
Modeling Proximity in Time

When we characterize a threat and assess its proximity, we can place that threat on a single axis—absolute proximity—with the current assessment at one end and the realization of the threat (that is, its occurrence) as the terminal point on the line. (see Fig. 13) Although occurrence is a static point on the axis, the location of the current assessed proximity will vary, moving closer to or further from the terminal point over time.

As with the DWN model, as a threat moves to the right along the time horizon, less time is available to act against a threat—there is less decision space. For example, continuing the military attack example, the forward deployment of forces to a border, the transportation and stockpiling of logistic materials, and a shift in national readiness may lead to an assessment that a threat is closer to occurring, shifting the proximity assessment to the right on the time horizon axis. Conversely, a drawdown of military forces, reopened negotiations, or cooling bilateral tensions may move the proximity assessment to the left.

Those seeking to provide warning can express the proximity of a threat along a proximity axis in several ways. Two basic options are to use a continuous spectrum of concern or to establish thresholds. The DWN WATCHCON system uses a threshold approach. A continuous concern spectrum will often be represented through color. This model provides an understanding of where a threat's proximity in time exists at any given moment. The next step is to understand a threat over time.

Figure 13. Threat Proximity Along a Spectrum.

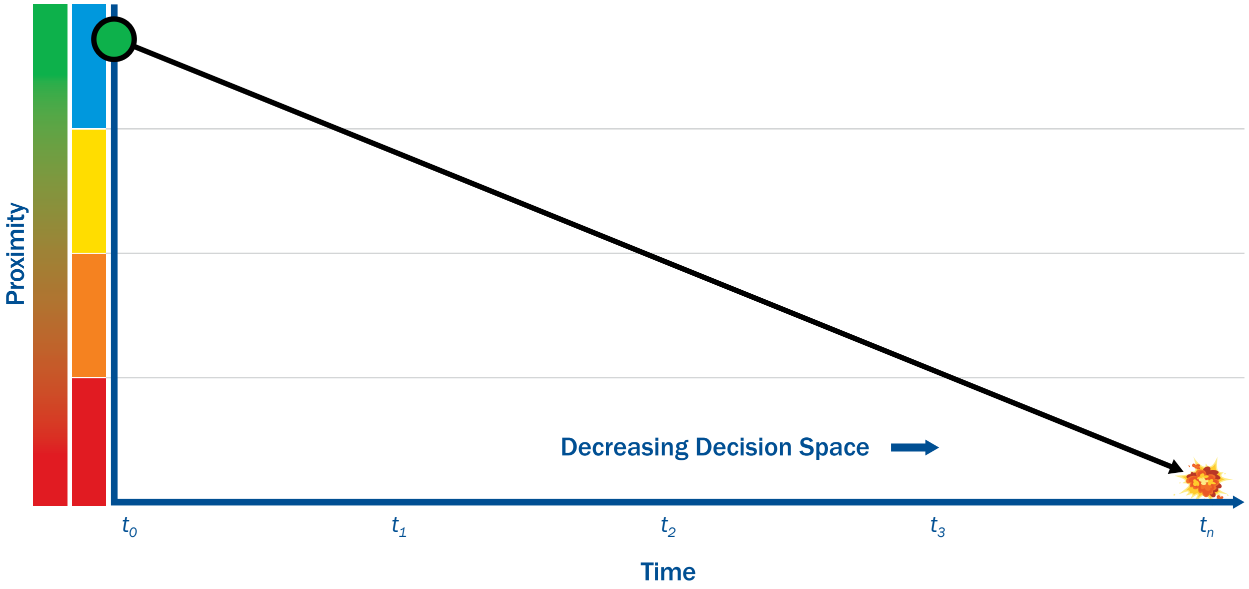


Author's figure based on the following sources: DOD IG, "(U) Evaluation of US European Command's Warning Intelligence Capabilities" (Redacted). https://www.oversight.gov/report/dod/evaluation-us-european-commands-warning-intelligence-capabilities.; Pitts, Russell, Defense Logistics Agency, Force Protection Conditions – A Tutorial, https://www.dla.mil/About-DLA/News/News-Article-View/Article/2740252/force-protection-conditions-a-tutorial/

Modeling Proximity Over Time

Expressing a threat's proximity over time requires a second axis to explicitly specify time in the model. By flipping the current model on its side, we can create a y-axis, then replace the x-axis with a timeline. The resulting two-dimensional space, with time on the x-axis and proximity on the y-axis, allows analysts and decisionmakers to visualize the path, or behavior, of a threat over time. The visualization of available decision space remains consistent with the current DWN model, and both threshold and continuous concern options can be used. (see Fig. 14)

Figure 14. Linear Progression of a Threat Over Time.



This example shows a linear progression over time, but other patterns are possible. Two potentially challenging situations are the rapid escalation and alert fatigue threat paths.[§§§] (see Fig. 15) On one end of the spectrum, a rapid escalation path is one where a threat's proximity remains stable, potentially for years, but then a massive shock or trigger event initiates a path of rapid escalation. On the other end, in the alert fatigue path, a threat quickly closes in proximity, but then remains stagnant for weeks, months, or even years. We might see this in a country with an economy that has been "one month away from collapse for the past three years."

Even more frustrating for many analysts or decisionmakers is the sinusoidal pattern of an annual military exercise path. In this pattern, all the indicators of an event may occur at regular or sporadic intervals, such

[§§§] Some warning practitioners use "alert fatigue" to express the drain on resources and readiness of maintaining a high-alert status or operational tempo in response to a potential or developing crisis. The dilemma is that, after an extended alert period when the threat does not materialize, the costs of maintaining that status become too high, but as soon as forces move off high alert, the attack occurs.

as with a recurring exercise that becomes more intense or realistic over time. (see Fig. 16) These patterns are expected as exercises provide a plausible cover for preattack capability, and repeatedly conducting one as realistically as possible creates a pattern of normalcy that can establish the conditions for surprise. This pattern can also occur with other threats, such as a volatile nation that seems to have one instability crisis after another over years, desensitizing analysts and decisionmakers to the next one (for example, "This is just another crisis of the month. We've seen this before, so there's no need to worry this time.")

Figure 15. Examples of Potential Threat Paths.

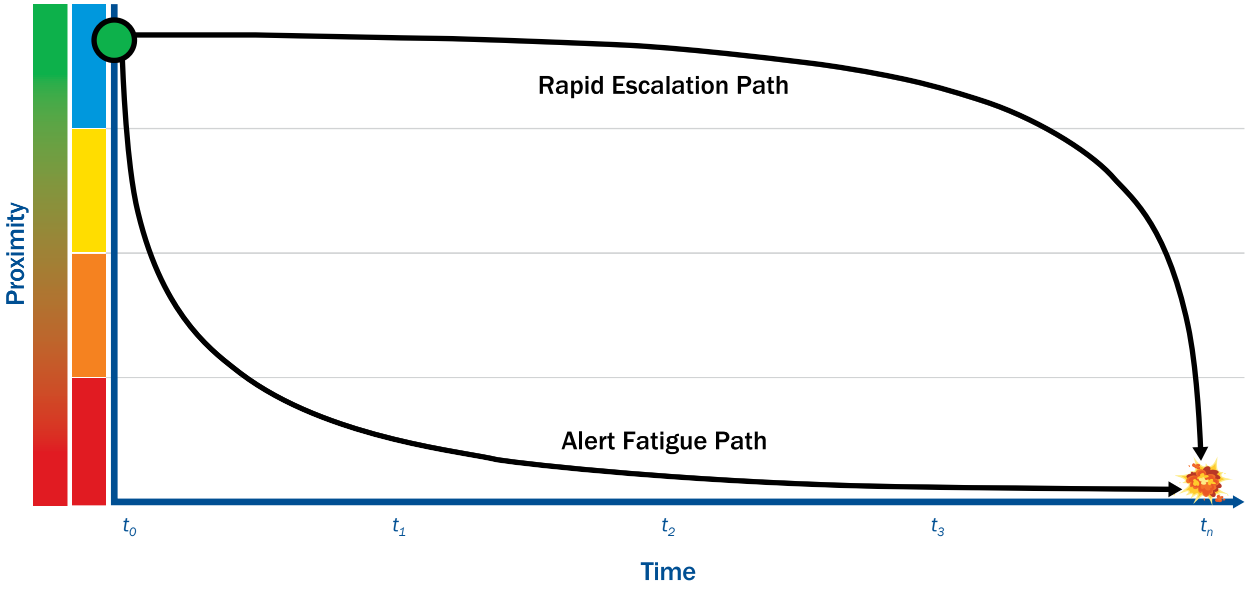
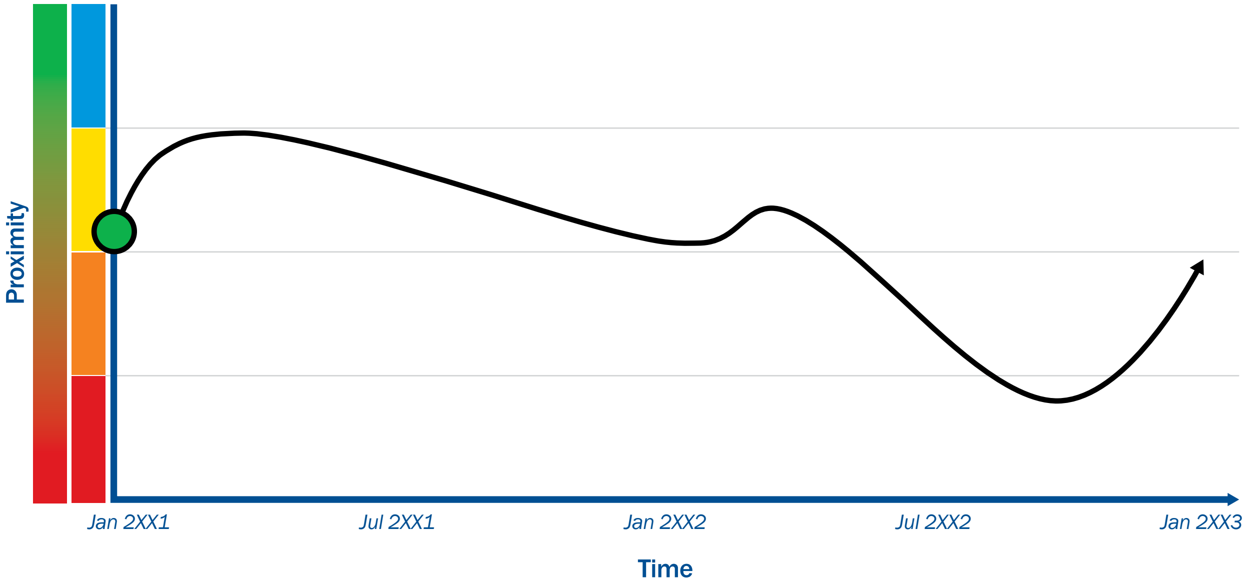


Figure 16. Each Threat Will Have a Unique Pattern or Signature Over Time.



Although these are examples of path archetypes that might occur, each warning problem will have its own distinct path over time. In the examples above, the time scale is both arbitrary and identical for each path. In practice, a true time scale will display the unique patterns and trajectories of individual threats, bringing distinctive challenges to each problem that must be understood by the analysts who monitor it and decisionmakers who must act in response.

Elements of Threat Characterization: Capability, Intent, and Ripeness

One final consideration for modeling and visualizing how threat proximity changes over time is to look at situations that have multiple proximity paths. For those threats—categorized by Michael H. as sudden hostile action—the ideas of capability and intent are highly relevant because we can consider them independently. For example, a nation may maintain a near-constant capability to engage in combat through forward-deployed forces, constant readiness, and rotating alert forces. The geopolitical environment, however, can be one in which neither side has a credible, near-term intent to attack. This status could describe the nuclear standoff between the North Atlantic Treaty Organization (NATO) and the USSR during the Cold War. Additionally, scenarios may exist in which one actor is assessed to lack a credible capability, but routinely threatens aggressive action and has a clear, long-term intent to disrupt the status quo. In each of these cases, the threat proximity based on intent may differ radically from the proximity based on capability.

This same concept can apply to other possible models of proximity to a threat. Referencing the rapid escalation threat path above, that curve could potentially be broken out into a capability or readiness curve, which might be maintained at a consistently low level as both nations work to avoid escalation, but within a tense environment where even a small trigger event could be the catalyst for extremely rapid escalation. In this case, the trigger event is the driver for a crisis, not the direct intent of either actor.

An important concept for dealing with threats when intent is not a part of the equation could be described as conditional ripeness,[225] in which all elements of a crisis or threat are present, but no reliable way exists to forecast which event might serve as a catalyst for a crisis. This will be especially challenging when dealing with threats that arise from collective action or from changes in the environment that fall in Michael H.'s category of tectonic shift.

Concluding Thoughts on Warning Models

At this point, one fair critique of this proximity-curve construct is that the model does not solve challenges in addressing issues such as capability versus intent. How does this advance warning? Similarly, how does modeling the threat landscape advance the discipline of warning? The answer is that the overarching purpose of modeling warning here is not to explicitly solve analytic or decisionmaking dilemmas. The purpose is to develop the explicit definitions, concepts, and models that form the basis of a full framework and theory of warning. An established theory enables future scholarly discussion, exploration, and research which can seek to solve identified issues and improve actual warning performance.[¶¶¶] It provides a basis for better understanding, discussion, hypothesis generation, and, eventually, resolution of the underlying problem. The impact of models on theory development will become more apparent as we turn to developing a theoretic framework of warning, which will employ the models presented above to illuminate the detailed elements of warning and the challenge of warning.

That challenge, broadly speaking for both the intelligence and decisionmaking communities, is building as robust a picture of the overall threat landscape as possible by identifying, characterizing, and triaging threats to determine which merit attention, then which of those should be reassessed periodically and which should be monitored constantly. For those threats that need to be monitored constantly, those enduring threats for which a decisionmaker has much less tolerance for risk or surprise, the challenge is tracking the threat's trajectory, accurately assessing the proximity over time, and working to avoid the pitfalls that certain path archetypes present.

That process, or more accurately the distinct tasks or elements that comprise it, will form a framework that completes our data-driven theory of warning, focused less on the types of events that surprise us and more on the nature of our surprise.

[¶¶¶] This is similar to the study of game theory. Modeling the conflicts inherent in a prisoners' dilemma, battle of the sexes, or stag hunt does not solve any of the problems they identify.

(Re)-Framing Warning

The strategic-tactical framework has arguably been the dominant warning paradigm across the course of the IC's history. In the past decade, the emerging-enduring paradigm has gained some degree of prominence to challenge or enhance it. Even more recently, Michael H.'s framework of surprise was a significant addition to the field and successfully placed emphasis on the nature of surprise, while tangentially addressing other theoretically significant ideas. None of these frameworks or approaches to warning, including their associated lexicons, are wrong. The strategic-tactical mindset has worked well for the defense intelligence and operational communities, and Michael H.'s work is essential reading for any analyst. It is possible, however, to develop a better and more comprehensive framework of warning that clearly articulates the full nature of the warning mission and, along with the definitions established previously, satisfactorily integrates all core theoretical elements of warning.

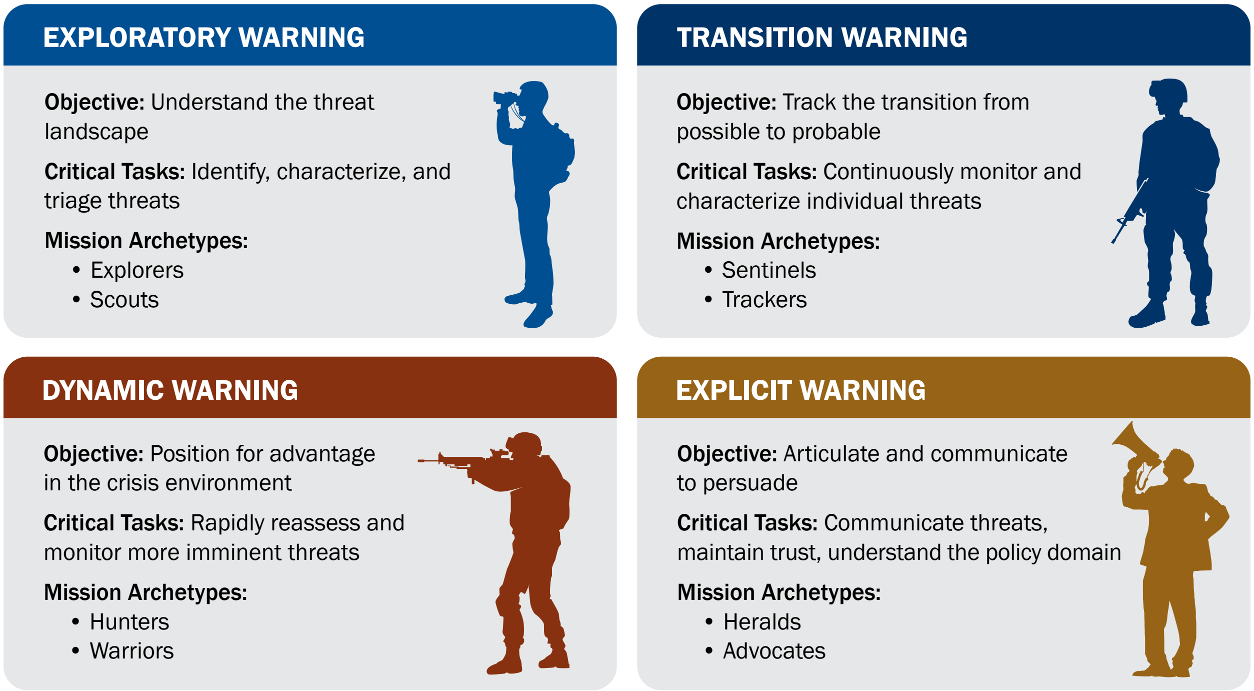
Because surprise is central to the mission and mindset of warning, it makes sense that any framework should operate from a perspective based on surprise. In contrast to existing frameworks which generally look at the types of events that surprise us or the nature of the surprise, this *Monograph* proposes a framework based on the way in which we experience surprise. This study's data and models revealed five incidences of surprise:

1. **Surprise at the very existence of a threat**: This is the purest form of the black swan threat that we either considered impossible or failed to imagine as a possibility. Combating this type of surprise requires us to *explore* the full threat landscape to *identify* threats.
2. **Surprise at the relative danger or proximity of a known threat**: This occurs when we either failed to understand significant changes in the threat landscape or to recognize that our characterizations of the threats were incorrect. It includes gray rhino threats. Combating this type of surprise requires constant *monitoring* and *triage* of the threat landscape to determine which threats to monitor and how closely.
3. **Surprise at the general timing and pathway of a threat**: This occurs when we fail to understand how a known threat is developing over time. We can be deceived by an adversary or fail to detect change over time due to the creep of normalcy. Failure can also occur when our attention is consistently drawn away by current or seemingly urgent matters. Combating this type of surprise requires detailed *characterization* and *monitoring* of individual threats over time.
4. **Surprise by the precise timing, location, and details of a threat**: This occurs—even when we are accurately monitoring a situation—when the fluid and time-compressed nature of a crisis environment or adversary deception creates excess noise in the environment. Combating this type of surprise requires a *dynamic* approach to warning with emphasis on speed and detail.

5. **Surprise despite warning**:[****] This occurs when intelligence organizations mistakenly concluded that they had provided a clear warning to decisionmakers, when decisionmakers were unpersuaded by intelligence, or when a general breakdown in the relationship disrupted the warning-response process. Combating this type of surprise requires *explicit* warnings delivered by trusted intermediaries to receptive decisionmakers.

Combating the following types of surprises and executing the full spectrum of the warning mission leads to a framework presented here as the "Four Functions of Warning," (see Fig. 17) in which each function is exemplified by a metaphorical archetype:

Figure 17. The Four Functions of Warning Framework.



EXPLORATORY WARNING

Objective: Understand the threat landscape

Critical Tasks: Identify, characterize, and triage threats

Mission Archetypes:
- Explorers
- Scouts

TRANSITION WARNING

Objective: Track the transition from possible to probable

Critical Tasks: Continuously monitor and characterize individual threats

Mission Archetypes:
- Sentinels
- Trackers

DYNAMIC WARNING

Objective: Position for advantage in the crisis environment

Critical Tasks: Rapidly reassess and monitor more imminent threats

Mission Archetypes:
- Hunters
- Warriors

EXPLICIT WARNING

Objective: Articulate and communicate to persuade

Critical Tasks: Communicate threats, maintain trust, understand the policy domain

Mission Archetypes:
- Heralds
- Advocates

Exploratory warning is the function of the scouts and explorers, tasked with fully exploring and understanding the threat landscape. This function counters the first two forms of surprise, affecting decisions on resource allocation and general strategy.

Once a threat is identified as a concern and has analytic or planning resources placed against it, the process moves to *transition warning,* which is the function of the sentinels and trackers. These individuals closely monitor specific issues or groups of issues to provide warning as a threat transitions from a possibility to a probability. This function supports decisions on when to begin responding to threats and when to begin

[****] While this term is not used in precisely the same manner as the original, it is taken from Betts's seminal article, "Surprise Despite Warning: Why Sudden Attacks Succeed."

implementing operational plans. It is where most defense warning has operated, focusing on applying scenarios and indicators against well-defined, enduring warning problems.

As a threat becomes more imminent or builds to crisis, a substantive shift occurs in the environment requiring a *dynamic warning,* which is the realm of the hunters and warriors. The decisions supported by this function include more detailed, tactical movement or responses, seeking to find advantage in the precise timing and preparation for a threat.

Finally, at all points in the warning process, a distinct need exists to understand the overall decisionmakers' environment and ensure compelling and clear communication takes place. This function is *explicit warning,* the realm of the heralds and advocates. These individuals lie at the intersection of intelligence and policy support, focusing on the relationship.

Any individual within an intelligence or decision-support community can take on a variety of roles over time, but they are likely to only be able to focus on or specialize in one or two functions. From an organizational perspective, offices or agencies should be able to understand who bears the responsibility for each function and how they manage the overall mission.

The foundational principles and framework here are focused on intelligence warning, but they could apply to a variety of fields. Doing so requires a more detailed look at each function.

Exploratory Warning: The Function of Scouts and Explorers

Exploratory warning seeks to maintain constant vigilance across the entirety of the full threat landscape, exploring to identify new and truly emergent threats and scouting known terrain to identify changes in that landscape. The defining model for exploratory warning is that of the threat landscape. Scouts and explorers focus on trying to better understand the landscape by scanning the horizon for new possibilities, scouting known terrain for changes in the proximity or importance of known threat issues, exploring the implications of changes to the landscape, and working to cover broad swaths of the terrain as efficiently as possible. Thus, exploratory warning counters surprise from not knowing about a threat or surprise about the relative proximity of a threat through the key tasks of *identifying* and *triaging,* which are arguably the most expansive tasks in the warning enterprise. Identifying new threats or possibilities can include the search for emergent threats arising from complexity, looking for new and potentially dangerous applications of known technologies, the development of new technologies, or significant demographic, economic, and social shifts. It also incorporates the disciplines of foresight and futures analysis. The triaging function contains two elements. The first is consistently looking for changes to the landscape by establishing baselines, then looking for discontinuities, anomalies, weak signals, or developing trends across a wide area. The second is understanding the implications for changes and identifying the potential impact on national security. Together, these analytic tasks provide a thorough understanding of the ever-changing threat landscape.

Exploratory warning enables decisions on overall strategy and resource allocation. With limited analytic resources and operational resources to explore, plan and prepare for, or respond to individual threats, the exploratory warning process aids in identifying those issues that warrant resources and those that decisionmakers might be able or willing to accept with a degree of risk. Not only can this type of warning affect operational planning and resourcing, but it can also help intelligence decisionmakers determine where to allocate scarce collection resources. That said, it is important to recognize that the full exploratory warning mission requires the IC to maintain some form of global coverage geographically and functionally. The tradeoff for intelligence decisionmakers is not in determining what to watch and what to ignore, but rather where to take a risk given the level of resources allocated or how to mitigate that risk.

All elements of the warning mindset are important for exploratory warning, but the most important principle is that of expecting change over time. Thus, the analytic techniques most applicable to exploratory warning are those that look for weak signals, such as change detection and horizon scanning. Additionally, the full scope of foresight and futures techniques are applicable. Exploratory warning also recognizes that either previous assessments can be wrong or the assumptions underlying them can be invalidated over time. Thus, devil's advocacy and the analysis of alternatives can be seen as elements of exploratory warning.

Ideally, successful exploratory warning allows decisionmakers to determine which contingencies are important or concerning enough to require developing plans, monitoring more closely, allocating (or reallocating) resources, or taking preventative action. When plans are developed against a threat or a decision is made to monitor a threat to reduce the chance of surprise, we move to the realm of transition warning.

Transition Warning: The Function of Sentinels and Trackers

Transition warning focuses on a specific issue to maintain constant watch and understand changes to that issue over time. It seeks to counter surprise at the general timing and pathway of a threat by deploying more detailed analysis and, usually, the indicators' method to track an issue in depth over time. The core theoretic assumption here is that once we have identified a threat as *possible* and decided to monitor it, that threat will transition to become a more probable event before eventually occurring.[††††] The function of the sentinels and trackers is to maintain watch on a specific element of the known threat landscape.[‡‡‡‡]

Transition warning informs and prompts the decisions that can or should be taken as the proximity to that threat shortens. Using the language of the DWN, transition warning protects decision space and

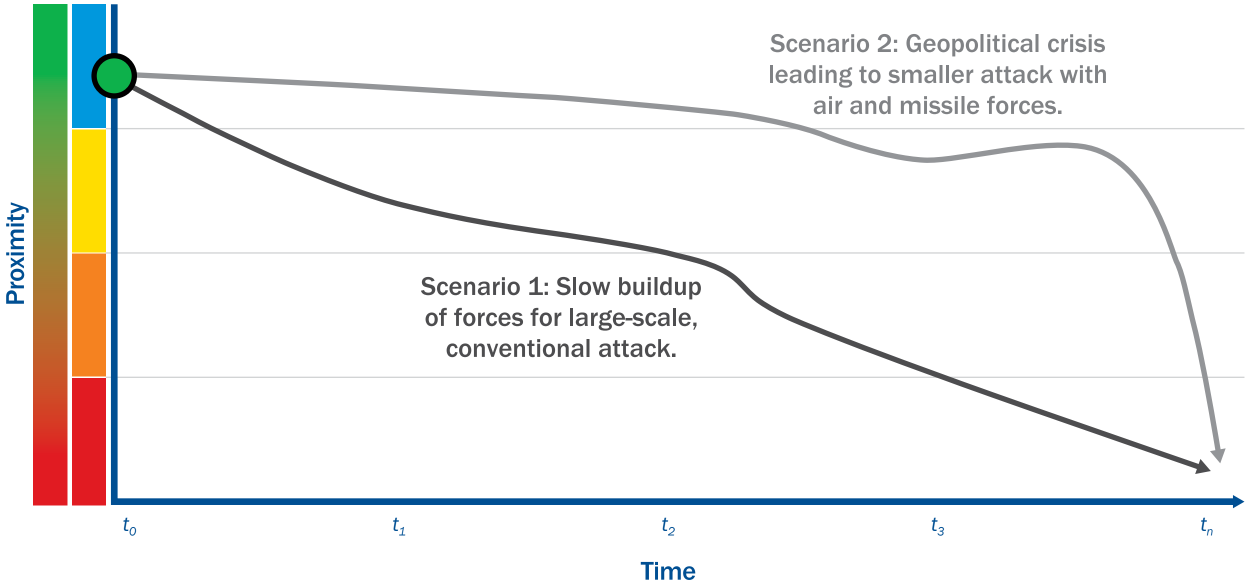
[††††] This can occur rapidly (i.e., rapid escalation). Scenarios in which an event moves from unlikely to occurring nearly instantaneously are usually impacted by a more stochastic external event, such as the unexpected death of a national leader, and can be considered "wild card" scenarios.

[‡‡‡‡] The metaphor of the sentinel in transition warning emphasizes the idea of a stationary watch on a specific element of the landscape, contrasted with that of the scout or explorer who looks across new or broader areas. The metaphor of the tracker acknowledges that a threat's path or nature can vary over time, requiring movement to follow and track the issue.

decision advantage within the context of a specific threat. Transition warning involves three key tasks. The first is understanding the possible evolution, progression, timing, and specific nature of a threat by generating multiple scenarios or hypotheses. The second is to use this new understanding to develop indicators that a threat is becoming more likely or more imminent. The third is to continually monitor those indicators to detect changes more precisely in proximity over time and to continually reevaluate the scenarios, indicators, and assumptions behind the analysis (that is, anticipating they will change).

Thus, as with exploratory warning, transition warning emphasizes the importance of change over time by trying to accurately assess changes to a threat's proximity without falling prey to the creep of normalcy, deception, or changes in the context of a threat. But the central tenet of the warning mindset relevant to transition warning is that of uncertainty and how it affects both analysis and communicating timely warning. Decisionmakers generally prefer warning as early as possible, but the earliest possible warnings are less certain. There is simply more time for things to change, and initial signals are generally open to multiple interpretations. If analysts or decisionmakers wait for more conclusive data to reduce uncertainty, they expose themselves to the risk of missing key decision points and, thus, being less prepared. When considered in terms of decision space, a paradox emerges. Warnings delivered when the decision space is ample will be more ambiguous and less likely to prompt action, and warnings delivered with a sufficient level of confidence to prompt action are more likely to occur when decision space is highly constrained.

Figure 18. Multiple Pathways to a Singular Outcome Can Exist.



Given the emphasis on proximity and time, it should come as no surprise that the model that explains transition warning is the proximity curve over time. (see Fig. 18) Understanding the possible evolution, progression, and timing of a threat translates into considering what type of path a threat's proximity curve will take over time and where that timing can be disrupted. This task involves asking questions, such as "are there specific steps that absolutely must be taken or events that must happen before a threat occurs, and how long do they take," and "are there any scenarios that could rapidly deteriorate or escalate?" In many instances, exploring different scenarios might indicate that several different pathways with radically different curves are possible.

This, in turn, might require developing indicators that distinguish between pathways. It might also prompt reconsidering the overall threat landscape and identifying pathways so different as to be considered separate warning issues. In the example above, the timeline, consequences, and supported decisions associated with Scenario 1 might be so different from those of Scenario 2 that it is best to consider them as two separate threats that require independent analytic efforts and indicator lists.

The proximity-over-time model also informs discussion on the timing of warnings—a critical consideration for transition warning. When do decisionmakers want or need to be informed about a threat, and what does that look like on the curve? Two potential options are to provide warning whenever there is a significant change in the overall trajectory of an issue (that is, a change in the analytic line "the situation is improving" or "the situation is beginning to get worse"), or when a threat reaches a threshold by meeting certain pre-identified criteria, such as with the DWN WATCHCON system. The pathway a threat takes over time can dramatically affect how those options function. Warning only when a threat crosses a threshold could limit the number of warnings given over time and create the illusion that analysts are not monitoring a problem. Meanwhile, warning whenever there is a slight shift in the analytic line could lead to too many warnings, desensitizing decisionmakers to future messages.

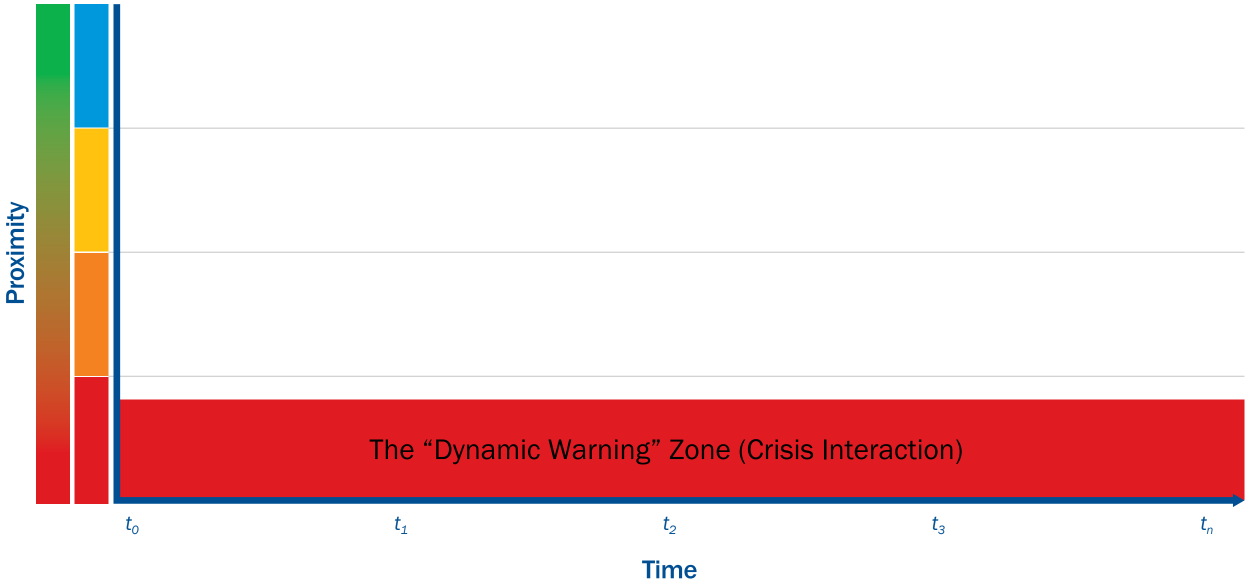
Ultimately, thinking through the possible trajectories of a threat over time and considering the needs of decisionmakers who require warning will answer the question of when to warn. The model itself does not provide the answer, but it does provide a way to visualize, discuss, and further theorize about what is necessary for successful warning.

Ideally, successful transition warning means that, as a threat approaches and becomes more likely, decisionmakers feel prepared and have taken the actions needed to either prevent the threat from occurring, ensure the costs of a threat are minimized, or posture to respond quickly. In the case of an internal stability problem, for example, decisionmakers may have no reliable options to prevent a crisis, but they may be able to ensure forces or materials are postured and ready for a response. At some point in the transition, however, something changes, and we enter a new function of dynamic warning.

Dynamic Warning: The Function of Hunters and Warriors

At some point in the transition from possibility to probability to occurrence, threats enter a categorically different phase of existence. This new phase is often defined by a crisis environment or an exceptionally fast-moving one where the cycle of decision and action becomes compressed. It can also be defined as one where analysis becomes less important than the collection of exceptionally detailed, actionable intelligence. This is the phase of dynamic warning, which exists in a subset of the proximity-over-time model. (See Fig. 19.)

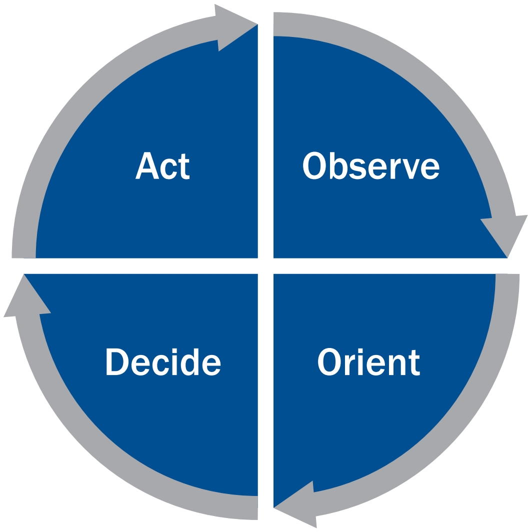
Figure 19. The Dynamic Warning Zone.



Dynamic warning seeks to inform the detailed decisions that will allow for the precise movement, positioning, and execution of plans or responses. It seeks to provide the detailed intelligence that enables decisive action, or what Dahl refers to as tactical intelligence in his Theory of Preventive Action. In the final period before a threat comes to pass, dynamic warning works to prompt and inform decisions on when and where to react. Usually, this occurs under conditions of crisis or imminence. Within the dynamic environment, deception is a renewed concern in the form of feints, diversions, or hidden movements to final positions.

While this framework does not use the term tactical warning, dynamic warning can generally be considered synonymous with contemporary interpretations of tactical warning. Within the dynamic environment, John Boyd's Observe-Orient-Decide-Act (OODA) Loop functions as the best model of the overall task of dynamic warning: (See Fig. 20.)

Figure 20. The OODA Loop as a Model of Dynamic Warning.



Author's figure based on: John Boyd, The Essence of Winning and Losing, 1995 (via archived version at https://web.archive.org/web/20110324054054/http://www.danford.net/boyd/essence.htm)

The challenge of the crisis environment generally is that of speed (that is, moving through the OODA loop faster than adversaries) to protect lives and resources. A second challenge, however, emerges when a threat sits at conditions of imminence for an extended period—forcing assets to remain on prolonged high alert. This can include operational forces awaiting an expected attack over a period of weeks or intelligence crisis management cells maintaining 24/7 analysis and production efforts. This challenge was modeled previously in the alert fatigue pathway. Two implied tasks arise:

1. To constantly look for positional advantage by moving troops out of harm's way before an attack, striking first, or engaging in last-minute diplomacy. This is the task of the warrior.
2. To maintain readiness, patience, and alertness. This is the task of the hunter.

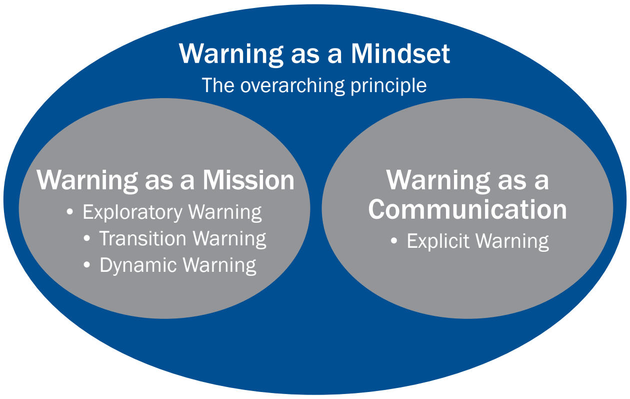
The end of the dynamic phase is marked by the actual incidence of a threat (for example, the moment of an attack or the start of a coup), or the successful management and disarming of a crisis. If a threat could not be deterred or disrupted, then it is the hope that dynamic warning provided decisionmakers with the means to enter the conflict with an advantage and minimize the losses and impact.

Explicit Warning: The Function of Heralds and Advocates

Explicit warning is *unique among the functions in that it exists simultaneously with the other three.* While exploratory, transition, and dynamic warning all follow the development of a threat from the moment it is recognized until it either occurs or ceases to exist, explicit warning focuses on the communication of warning to specific decisionmakers in such a way as to enable decisions and actions across all other functions. Referencing the three core definitions of warning previously proposed, the exploratory, transition, and dynamic functions constitute warning defined as a mission, while explicit warning constitutes warning defined as a communication. The warning mindset, meanwhile, is the condition needed to successfully execute all four functions and is arguably the defining feature of warning as a distinct discipline. (See Fig. 21.)

Explicit warning does not support any one type of decision. Rather, it supports all decisions by seeking to ensure those decisions are prompted. The challenges posed by this function go far beyond simply ensuring a message reaches a decisionmaker, although it is often daunting enough given that time and attention are exceptionally scarce resources for many key decisionmakers. The biggest challenge to successful warning will often be that the messages presented run counter to a principal's policy interests, desired outcomes, focus areas, or worldview. In other words, how do you deliver bad or unwanted news and prompt a difficult decision without being dismissed from the room or simply ignored?

Figure 21. Linking the Four Functions of Warning to the Three Core Definitions of Warning.



Answering this question is the task of the heralds and the advocates. These roles are focused on the communication of messages, which includes crafting messages in a way that decisionmakers can clearly grasp, understanding the context in which the message exists, and knowing the best route for a communication. Heralds ensure a message is heard and understood, which does not mean shouting (literally or metaphorically). Rather, messages that meet this criterion are expressed clearly, convincingly, and in language familiar to the recipient. This is the art of creating compelling narratives that prompt decisions but do not dictate or recommend specific outcomes. Advocates focus on understanding the context in which the message exists and understanding the best route for a communication. The advocate does not argue for a specific outcome, but rather advocates on behalf of the decisionmaker being warned. Advocates understand the policy space in which a warning exists, including where it lies in the decisionmaker's priorities and how the decisionmaker understands the issue. Doing so enables them to understand what decisions might be made in response to a warning and, thus, tailor the warning for greater impact. Sometimes the best advocates may not be from the intelligence side of the equation but may instead be a trusted member of the decisionmaker's inner circle or someone with whom they share a background.[226] Sometimes it can be someone able to speak the decisionmaker's language more readily. When individuals outside a person's social group, tribe, or background present warnings, or when warnings are expressed in unfamiliar terms, they may not be trusted or understood.[227]

As with many elements of intelligence, trust is the advocate's ultimate currency. The best advocates or heralds might not be those who consider themselves part of the warning process: intelligence briefers. Part of an intelligence briefer's task is to develop trust with their principal, and the briefer's ability to determine what is communicated and what gets emphasized makes them key elements of the communication chain.[228] Additionally, they develop a better understanding of the principal's style, interests, and priorities than most line analysts or dedicated warning analysts are likely to possess. While there is a degree of romanticism in the idea of the warning officer whose job is to bravely walk into a room and honestly present disconcerting information on a looming threat, the efficacy of this approach may not justify the role. Perhaps the best thing a herald can do is understand when it is necessary to hand off the warning to an advocate.

Finally, the notion of explicit warning emphasizes a key element of the definition of warning as a communication. Namely, communications should be directed toward a specific decisionmaker or group with the ability to act on a warning. This means that explicit warning cannot be fully achieved by pushing analysis out in a standard product, hoping that it is received and understood as a warning by the policy community. Mandating that the warning message or language be included in an analytic tradecraft statement or closing paragraph (usually more of an insurance policy against accusations of not having provided warning than a genuine effort) essentially abdicates the role of herald or advocate. These types of products, even if considered warnings by their authors and producing offices, instead hope to function *as a warning.* These types of products fall under the broader category of intelligence which seeks to inform the worldview of the decisionmaker more broadly. This is still an important role for intelligence, and, in some instances, it may be all that is needed when the intent is to broach the subject, or keep an issue fresh in the decisionmaker's mind, to make expected future warnings more effective and understood. In these cases, there is still an explicit intent to support a warning.

While warning is a mission and a mindset, it is also a communication in the context of the relationship between intelligence and policy or operations. Remaining mindful of the role of explicit warning ensures analysis has more impact than if it were considered only in the analytic functions of exploratory, transition, and dynamic warning.

Individual Applications: To Specialize or Multi-Class?

It is unlikely that any one person will fill the roles of every single archetype, but it is likely that nearly all intelligence personnel who deal with analysis or warning will feel a connection with at least one of them. Ideally, even individuals who do not immediately think of themselves as intelligence or warning analysts will identify with one or more of these roles. Consider futures professionals or scholars looking to form projections decades into the future who see themselves as explorers at the most extreme edges of what the threat landscape might look like.

One decision that organizations will need to make is whether individual analysts will specialize in one function or attempt to "multi-class" and execute several functions at once. At the individual level, it is more efficient if one person can effectively accomplish multiple functions. Doing so, however, may mean they lack sufficient training or experience in any one area. Just as with many popular tabletop role-playing games, individuals almost certainly will need to function as part of a larger team, ensuring their skills and abilities overlap to accomplish the mission. Although the choices of individuals matter, the biggest challenge will be in how organizations manage individuals within teams to accomplish the full warning mission.

Organizational Applications: Bringing It All Together

An organization using this framework does not necessarily need a dedicated warning office to conduct all four functions. Instead, organizations should understand for which functions they will be responsible and explicitly establish their own policies and procedures to accomplish those parts of the warning mission. This can mean distributing functions between different offices. For example, many all-source organizations have a separate office that manages executive briefing functions. These offices and individuals clearly fill the explicit warning function. Leaders at such agencies and offices need to ensure that briefers understand their roles as advocates and heralds and that mechanisms exist to provide relevant feedback from principals to line analysts, as well as ways for analytic leaders to highlight and emphasize warning messages to be delivered to specific decisionmakers.

Some organizations may determine they fit within one role more than others. Alert centers and intelligence watches may have a role to play in transition warning, but they will be more likely to identify with the tasks and functions of dynamic warning. Likewise, individual teams and branches may be tasked or decide to focus on exploratory warning or transition warning. No individual office needs to singularly accomplish all four functions as long as an agency-wide strategy or policy are in place that ensures all four occur.

The ideal execution of the four functions framework will see decisionmakers continually informed and making key decisions against threats in time to act. This starts with a decision to form a response plan to a developing threat identified by scouts or explorers, then moves to the decision to implement that plan prompted by sentinels and trackers. Finally, the "go order" is given, enabled by exquisite collection and warning from a hunter, with the warnings at each distinct phase presented convincingly by heralds and advocates. Ideal execution will also ensure strong relations exist between intelligence and policy teams, tailoring messages and analysis to the needs of the policymaker, while also incorporating intelligence to understand the overall policy space and its implications.

The framework presented here is a holistic approach to warning. In addition to offering applications to both individuals and organizations, it presents ideas to consider in debates in warning and future research and scholarship.

This page is intentionally left blank.

(Re)-Thinking Warning: Opportunities and Implications

The definitions, models, and framework presented in the preceding pages form an initial, comprehensive theory of warning, grounded in data from the literature and the experience of practitioners. In addition to providing a thorough lexicon of warning, from specific definitions of warning to concepts, such as proximity, and the functions of the warning mission, this theoretical approach incorporates the seven fundamental principles of warning established earlier. The idea that warning counters surprise is captured through definitions and a framework built on how we experience surprise. The warning mindset is captured in a specific definition. The idea that warning must be timely and account for time is specifically modeled in the proximity curve over time. The complete nature of the warning mission is encapsulated in the four-functions framework. The need to convince or persuade decisionmakers is included both in definitions and, more important, in the specific function of explicit warning. The importance of the relationship between intelligence and policy is also captured in the function of explicit warning (implying that this function and element of the warning mission might be the most important, even though many intelligence professionals see warning as largely analytic).

Opportunities for Continued Research and Development

As a theory of warning, the themes and resulting concepts presented here are not intended, by themselves, to conclusively solve challenges or end debates about warning within the intelligence and wider national security communities. Rather, they serve as a common starting point for the development of agency- and issue-specific solutions, informed discussions, and continued intelligence research and scholarship. Several prominent opportunities exist to extend the overall literature on warning and the models developed here, as well as to fill potential gaps:

Opportunity Warning

It seems fitting to propose that the first opportunity for expanded research, as well as possible framework development, is to further explore and define *opportunity* in relation to warning. An increasingly frequent idea in both the literature and among practitioners of warning is that warning analysis should consider and present opportunities to mitigate threats. In the most prominent example, Gentry's reframing of intelligence failure includes opportunity warning alongside threat warning.

There is, however, a need to better define the precise relationship between threat and opportunity. For example, is an opportunity within the warning context defined as an action that specifically reduces the anticipated costs or probability of a threat, or can opportunities exist within warning as the means to achieve preferred outcomes rather than just avoid costly outcomes? Should the idea of opportunity warning be formally adopted and developed by organizations such as the DoD's DWN? Finally, do the methods and mindsets associated with traditional threat warning apply to opportunity warning, or are there distinct methods and modes of thinking for approaching opportunities? Ultimately, the path to resolving these questions reinforces the idea of warning as a social construct. That is, the answer will largely be determined by how IC agencies and individual offices choose to view opportunity warning.

Threat Theory

Considerable time and attention were dedicated here to defining warning as a mission, a communication, and a mindset. The definition of a threat, however, needs further exploration and refinement. Research is needed to better explore how analysts and decisionmakers think about and characterize threats. Existing literature is worth exploring, but the topic is ripe for a more detailed exploration using grounded theory to understand exactly how members of the IC and broader national security community consider threats and triage them. Specific methods and models for triaging threats also need further consideration. This can be seen as another form of filtering the signal of priority items from the noise of issues demanding decisionmaker attention. An excellent example of an initial framework for guiding decisionmakers exists in Clarke and Eddy's Cassandra coefficient.[229]

Warning Analysis Methodology

The dominant structured analytic methods for warning—scenario generation and indicators—are powerful tools, but they still require development. This study originally intended to focus on methodological issues in warning, such as filtering through competing ideas on what makes a good indicator, the applicability of indicators to issues other than military attack (or any form of sudden hostile action), the integration of social science methodology and statistical research into warning, and a more thorough critique of the established DoD methodology. It quickly became evident, however, that exploring these issues was a secondary concern to forming a stronger core understanding of warning on which to base further research. Thus, the issues originally intended for study still need attention. Additionally, a methodological study in the context of the four functions of warning can now explore what are the best techniques not just for warning but, specifically, for exploratory, transition, dynamic, and explicit warning. In the case of explicit warning, the methodology may be less analytic and instead focus on the best ways to convey proximity, risk, and overall warning messages persuasively. The research of Meyer et al. stands as the seminal work in this topic and a starting place for research.[230] A second possible approach is to look at warning by individual issue (for example, internal stability, military attack, economic collapse, or pandemic disease) and explore optimal methods or indicators for each specific subject.

Understanding Surprise

The full literature on surprise in national security needs exploration outside the subject of surprise attack to compare how various models or theories of surprise either reinforce, refute, or revise the idea of surprise presented here. Specifically, an opportunity exists to either expand or critique the idea of defining functions of warning based on how we experience surprise. Like the research methodology employed to develop Michael H.'s typology of surprise, a comparative case study exploration of how we experience surprise can better inform and define exploratory, transition, and dynamic warning. For an example of how this differs from Michael H.'s taxonomy, consider the attack on Pearl Harbor, which falls into his category of sudden hostile action. From the perspective of how we experience surprise, however, the issue becomes somewhat more complicated. The idea that the Japanese would initiate an attack that would expand the conflict and draw in the United States was well established, so a Japanese attack was expected. Even the timing of the threat was generally well known. One could argue that the real surprise was simply the initial target, Pearl Harbor. To the contrary, one could also argue that the actual surprise was that Japan had the capability to successfully launch an attack. How would one categorize the surprise (or surprises) at Pearl Harbor or any other existing case study from the literature? The objective of a research program looking at how we experience surprise would be to develop a typology and better understand how analysis or warning might counter different types of surprises, following the example laid out by Michael H.

These are just a few of the most promising opportunities to expand the literature on warning. Other potential avenues include exploring the private sector and academic literature on risk management and expanding the academic study of intelligence success. Much room exists to further develop the framework presented here into a more complete form (for example, is it possible for tasks to merge, or is there any assumption of progression from exploratory to transition to dynamic warning?).

In the meantime, there are implications from this study's findings for current debates regarding warning in intelligence.

Implications for Key Debates

Is Every Analyst a Warning Analyst?

One of the most contentious debates about warning within the IC focuses on who is and is not a warning analyst. More specifically, is every analyst a warning analyst, or does it require a special skillset that is inimitable to a subset of the analytic cadre? Grabo's exploration of warning identified several characteristics deemed essential to a good warning analyst. These included both basic intellectual abilities and specific "attributes of character or temperament," such as interest and motivation, a capacity for hard work, initiative, a willingness to risk being wrong, and an indifference to rewards and appreciation.[231] Gentry and Gordon concur with

Grabo's emphasis on a special character of warning analysts, stating that "virtually all warning specialists in government and business, and students of deception, argue that there is something special about the personal characteristics of successful practitioners of strategic warning and deception. They find that few people make good warning analysts." They later noted that "most of the US IC rejects these insights [that only certain people are good at warning and deception], however."[232] What Grabo, Gentry and Gordon, or others have not demonstrated, however, is how the desired talents and outlook of an ideal warning analyst differ from what is desired from any member of the analytic cadre, or any profession that relies on critical thinking to make inferences from incomplete data. So, from the perspective of a desired skillset, no satisfactory argument identifies the existence of a major distinction between analysts and warning analysts.

When we consider the definition of warning as a mission and the warning framework provided above, virtually every professional throughout the IC should be able to identify with one or more roles. Indeed, one would be hard pressed to find a good analyst who would persuasively argue that the definition of warning as a mission differs significantly from their core analytic duty. From this perspective then, it might appear that every analyst has significant warning equities in their job.

So, if it is not the personality or the task that is clearly exceptional, why is warning seen so adamantly by its practitioners as a distinct specialty? The answer, alluded to several times, comes down to the understanding of warning as a mindset.[§§§§] Those who excel at warning—in addition to exemplifying the desired attributes of a good analyst—are likely to be predisposed to think in terms of possibilities over probabilities, exhibit a contrarian point of view, or work in an environment that emphasizes the warning mindset. So, the ultimate determinant of whether every analyst can be a warning analyst comes down to whether every analyst can easily adopt a warning mindset.

The warning mindset is arguably not the default for many professions. Although foresight practitioners and futurists focus on the inductive thought process of creating multiple scenarios, the primary thinking process for many analysts is deductively focused on accurately forecasting and identifying the most probable outcomes. The objective is to reduce the uncertainty that decisionmakers face and provide accurate forecasts (not predictions). The question, then, is whether all, or even most, analysts can switch between the standard and warning mentalities as needed. Here, evidence from the psychology of intelligence suggests that the answer is no.

Truly good analysis of alternatives and devil's advocacy requires challenging the mindset that established an assessment. Mindsets, as Heuer pointed out, are quick to form but resistant to change.[233] This sets up a contradiction of sorts. A mindset is needed in reference to a problem so that our minds can filter

[§§§§] The term "mindset" should be understood as a set of mental models that form our understanding of how the world functions. As described here, mindsets can vary in scale. A "warning mindset" or a "growth mindset" are examples of broad mindsets about the nature of the future or of personal development, respectively. More specific mindsets form around individual issues, however, affecting how we interpret the actions of national leaders or understand national power. Thus, a single individual can have multiple mindsets in operation simultaneously. For more specific issues, it may be easier to mentally switch terms and think of *frames* or *lenses* through which we view an issue.

information, conduct analysis, and establish an analytic line, but the very act of creating a mental frame, even before coming to an analytic conclusion, hardens analysts and organizations against challenges to that frame. Stated another way, the process by which an analyst arrives at an analytic conclusion or establishes an analytic line automatically makes it more difficult, although not impossible, for that same analyst to effectively challenge that assessment and consider other possibilities.

There are two ways to potentially overcome this contradiction and establish an analytic cadre capable of establishing analytic lines, while also challenging them and exploring other options. The first is training and education, and the second is an organizational emphasis. The debate on intelligence training and the ability to change individual modes of thinking is beyond the scope of this study. Those who assert that a warning mentality is simply a "you have it, or you don't" characteristic, which cannot be trained or cultivated, would do well to consider Carol Dweck's research into growth and fixed mindsets, which suggests that it is indeed possible.[234]

The most important implication for warning from this research is that the overriding requirement for every analyst to function effectively as a warning analyst is the ability to adopt the warning mindset to identify new and emerging issues, challenge assumptions and existing analytic lines, and provide the detailed tracking of high-priority issues. Therefore, it is possible for every analyst to function as a warning analyst. Every analyst also has definite warning equities in their work. The question then transitions to the units of analysis above the individual analyst, the teams, offices, and agencies in which these analysts work along with their associated missions and norms.

Warning Organizations

Assuming for a moment that enough individual analysts can develop and reliably employ a warning mindset, the subsequent question is whether every analytic *unit* can match that effort. While the idea of EAAWA calls out the "analyst" on the individual level, overall production processes and priorities are set at the branch, division, and office levels. In a parallel to Gentry's and Gordon's taxonomy of institutions, the question now is how well can the "every branch is a warning branch" system function?

The evidence points much more strongly to the argument that mainline intelligence units are unlikely to sufficiently accomplish the full warning mission with an adequate warning mindset. A variety of incentive structures are in play, discussed throughout the intelligence and warning literature, which point to this conclusion. The first is the overriding tyranny of the now, which focuses many teams and individual analysts on current intelligence because of the overriding demand from customers for products that fit this category of intelligence.[235] Additionally, organizational incentives for production and publication—particularly in office cultures where better numbers lead to a better review and promotion potential—have the potential to reinforce production that aligns more with current intelligence than warning. Finally, organizations need to establish set analytic lines. Even if we assume there is no pressure to maintain that analytic line or no resistance to routinely challenging it (a very poor assumption at best), the contradiction previously discussed comes into play. Therefore, the idea that every branch is a warning branch can succeed is not promising, and the idea that every analyst can be a warning analyst is not well supported.

So, what other options exist for organizational structures to perform better? Looking at the other end of the centralized warning spectrum, dedicated warning analysis teams are likely to be more successful at considering possibilities and embodying the warning mindset. As Gentry and Gordon point out at length, however, a completely different set of organizational and incentive challenges exists that makes successful warning difficult.[236] Meanwhile, they offer hybrid warning structures as a potential "best of both worlds" solution, but even those will experience territorial issues and often require a level of tasking authority, executive access, and receptivity that is unrealistic.

One possible solution to the organizational challenge emerges from the principle that warning depends on the relationship between intelligence and decisionmakers. Rather than focusing on warning as an intelligence-driven process, Clarke and Eddy present the idea for a formalized national warning office within the Executive Office of the President, placing the function at the central hub of national decisionmaking. As they envision it, "this small, elite team should not be, as was [the NIO[W] for Warning's office], part of the IC. Rather, the office would have a broad, even intentionally vague, mandate to look across all departmental boundaries for emerging threats."[237] This proposed solution focuses efforts on exploratory warning and, by its placement within the White House, explicit warning. It is unclear if and how it would manage transition or dynamic warning efforts, and such an office would also be likely to face most, if not all, of the same challenges that intelligence warning organizations face.

Although a national office of warning may not be tenable, multiple possibilities exist for dedicated organizations, teams, task forces, or processes that specifically link intelligence and decisionmaker elements at lower levels, collaborating to develop tailored warning messages that can be communicated through intelligence reporting, operational channels, or both. DoD may prove instructive in developing this style of organization based on interactions among intelligence, planning, and operational teams, and elements of military doctrine that mix intelligence and operations in a unified process such as targeting.[¶¶¶¶] Within this construct, it may be fruitful to define those who specialize in warning as mission managers who understand the full mission, coordinate efforts that occur across the analytic cadre, and have authority to task on occasion and push for applying the warning mindset to an issue. At an organizational level, a key question senior leaders must address is how to allocate their overall production, bending to the incessant demand for current intelligence and more tactical products, or emphasizing and rewarding efforts to provide exploratory warning and develop relationships with policy and decisionmaking principals.

Meeting Every Analyst's Responsibility for Warning

Every analyst across the IC has a responsibility to provide warning, and even if they are not crafting direct, explicit warning products, the products they create often have the capacity to serve as a warning. Given how significant the overlap is between many intelligence products and the exploratory, transition, and dynamic functions of warning, this *Monograph* argues that all analysts have significant warning equities

[¶¶¶¶] The DoD doctrine for targeting is 3-60, which indicates it is "owned" by the J3 and the operational community, even though intelligence analysis is a major element of the process.

in their work. Enabling the warning function at the individual level then becomes a matter of training to develop, reinforce, and maintain the appropriate mindset. But, even if the community succeeds in doing so, analysts will still need to find acceptance of this mindset and mission at the various organizational levels within agencies and offices.

Thus, the most significant challenge to successfully executing the warning mission exists in the task of creating an organizational structure—along with supporting procedures, products, and practices—that balances the primary mindset of intelligence analysis and production with the warning mindset. Although every analyst may have warning equities, a very strong case can be made against the idea of EAAWA as an organizational construct. Relying on the standard analytic and production mindsets and processes to provide warning risks repeating failures of the past. Some form of specialization, focus, and development is needed to enable the broader workforce. Dedicated offices, hybrid offices that manage the warning mission, or organizational champions are all possibilities for the future. This effort can learn from the model of analytic methodologists and tradecraft specialists within the IC. Although every analyst has a responsibility to maintain the highest standards of the profession and incorporate structured methods into their analysis, the IC has found value over time in promoting a dedicated cadre of individuals who specialize in the warning subject both formally and informally. The essential factor is to ensure someone is focused on enabling the warning mindset across all functions of warning.

The Warning Renaissance: Challenging Paradigms and Exploring Ideas

This *Monograph* set out to advance the art and science of warning to encourage and inspire new thinking, new research, and new discussions on the topic. The science side of the equation is represented by using a rigorous, data-based research methodology, creating a formal framework and definitions, and developing formal models of specific ideas. The art side of the equation is represented by the specific data sources selected for study, specifically the impressions of both contemporary and historical practitioners of warning, drawing from their career experiences. The art of warning is also expressed through the concept of warning as a mindset, which may be the defining element of what makes warning an art of sorts.

Time will tell if this work inspires continued research or a true renaissance, but part of the process of scientific or intellectual advancement means challenging established paradigms and assumptions. The contribution of this research in challenging established norms is to argue that definitions of "strategic warning" and "tactical warning" need to be dismissed as terms of reference in favor of a lexicon that defines warning as a mission, communication, and mindset alongside the four-functions framework.

In closing, it is worth moving one level deeper to ask if the result of this research also challenges one last foundational term of art, the actual word "warning." Part of the argument presented above for dismissing the terms strategic and tactical warning in favor of a new primary lexicon is that these terms can create confusion, often come with inherent assumptions or intellectual baggage, and can create unnecessary divisions of effort. A strong argument can be made that the term warning itself suffers from the same flaws.

Additionally, if we emphasize or view warning as the intersection of intelligence and policy, and if we emphasize the importance of the relationship between intelligence and policy, then the argument can be made that the term warning is insufficient to capture the character of this nexus. Finally, the idea of opportunity warning can seem a contradiction in terms to many people, given that warning is sometimes explicitly defined in reference to negative outcomes and often connotes negative outcomes. If the IC wants or needs to embrace opportunity analysis as part of what we currently consider warning, then perhaps using the term warning holds us back. Such detailed critique over the specific words and terms we use may seem pointless to some, but the words we use can affect how we think about issues.[238, 239] If the IC's desire is to be as effective as possible at countering surprise—prompting and persuading decisionmakers and protecting national security in doing so—then it becomes necessary to consider the words with such scrutiny. The idea of intelligence support to risk management may be a better overall descriptor to integrate the idea of managing surprises while searching for opportunities.

Regardless of what the future holds with respect to terms, the topic of warning warrants continued research, debate, and scholarship. It is, by any name, a critical element of intelligence and national security with a rich landscape ripe for continued exploration.

Acknowledgements

This *Monograph* is the culmination of nearly two years of direct focus as part of an NIU research fellowship and several additional years of work experience and formal education. It would not exist without the amazing support of a huge cast of friends and colleagues. Sufficiently thanking every person who has helped me along this journey would undoubtedly take more space than the preceding research, and I would undoubtedly forget to mention somebody. All my career professional colleagues, my friends, and my fellow scholars at NIU have had a part in making this happen, and I would like to express my sincere thankfulness and appreciation to them all (if I've ever talked to you about warning, you've had a role in this project). There are several individuals, however, who warrant a particular note of gratitude.

The faculty and staff of NIU have been instrumental in making this work a reality. I am appreciative of the many students I've had an opportunity to teach for being able to present early findings and ideas and gain feedback (especially since being a captive audience often meant they didn't necessarily have a choice in the matter). In addition to all the faculty members I've interacted with, my fellow warning instructors Ken G., Jay H., and John S. deserve special mention, as they are some of the most well-versed individuals in the subject and most influential voices to me. Within the Office of Research (OOR), every single person has been a tremendous inspiration and help. I'm grateful to Manolis Priniotakis and Stacey Pollard for their leadership and encouragement within OOR, and especially to Jennifer Davis for her mentorship, encouragement, and friendship, which helped me get past the most challenging parts of this process, find my confidence, and come into my own as a researcher and scholar. I've been the beneficiary of the amazing experience and knowledge of Dr. Phuong Hoang, Dr. Deb Pfaff, and future Ph.D. Chris Ventura. Chris's early work at NIU dealing with Gray Rhinos is what introduced me to that entire literature. I am especially indebted to my committee reviewers, Josh Kerbel and Frederic Baron. I've had the pleasure of working with Josh for several years, and his example has always been an inspiration to me to challenge the status quo and push the IC to become better. As my primary reader, Frederic provided the most detailed feedback on this project, dramatically improving the final product. Lace Frazier has been a wonderful source of encouragement, and as the executive assistant for OOR, she is the one who makes the show run and the holder of all the answers to "how do I" questions. All my fellow fellows have been tremendous colleagues during the past two years, with particular gratitude to Eli M. for many deep discussions on warning and intelligence and Julie F. for being the person I could always confide in for an "am I the only one who feels lost or out of my depth here?" moment.

NI Press has been an exceptional team to work with, and the most important unsung hero of my fellowship has undoubtedly been LeeAnn Scheuer. I'm not a great writer. I'm a decent writer with an amazing editor,

and LeeAnn has also been my cubicle neighbor for two years, suffering through constant distractions, interruptions, questions, and "does this sound okay to you" queries.

My colleagues Annaliis C., Caroline B., and Andrew H. deserve special recognition for both their friendship and early feedback on my research. Within my previous office in the Joint Staff, I'm grateful to Jimmy Y. and Paul B. for their exemplary leadership and willingness to think critically about warning and make it a central part of their mission. I am also grateful to my entire chain of command from Kevin T. to Fara B. and Jeff C. for their willingness to let me go off for a year (and eventually two) to pursue this opportunity. I'm indebted to all my colleagues in the warning branch over the years for their dedication to mission, for teaching me so much through our interactions, and especially for taking on the extra work incurred when a person departs the office for a joint duty assignment.

My entire fellowship experience would not exist without the guidance and encouragement of Miriam Z., who helped coach and mentor me to better understand my goals, and who set me on the path that led to my application to NIU.

Finally, the support, friendship, encouragement, instruction, help, and love I've received from colleagues over the years is ultimately dwarfed by that I have received from my family. My wife, Robin, has been a source of constant encouragement throughout this time (and for many years prior), and I'm truly grateful for the sacrifices she's made so I could endure longer commutes, later hours teaching, and several home hours hidden away trying to write. My daughters, Megan and Emily, have also sacrificed to make this happen, and while they haven't necessarily been happy when Daddy wasn't coming along on a vacation or thrilled at me being gone during evenings teaching, their understanding and love (especially hugs) have been unending. I owe them quite a few board game evenings and pool trips.

Appendix A: Extant Document Data Collection Bibliography

Bar-Joseph, Uri, and Rose McDermott. *Intelligence Success and Failure: The Human Factor* (New York: Oxford University Press, 2017).

Betts, Richard K. "Analysis, War, and Decision: Why Intelligence Failures are Inevitable," *World Politics* 31, no.1 (1978): 61–89.

Betts, Richard K. "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly* 95, no. 4 (1980–1981): 551–572.

"Conference Proceedings, Strategic Warning in an Evolving Threat Environment," *Studies in Intelligence* 62, no. 4 (2018).

Clark, Keith. "On Warning." *Studies in Intelligence* 9, no.1 (1965): 15–21.

Cozad, Mark, and John Parachini. "Strategic Warning: Organizing and Managing the Mission for the Current Era," *Center for the Study of Intelligence,* 2017.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013).

Davis, Euan G. "A Watchman for All Seasons," *Studies in Intelligence* 13, no. 2 (1969): 37–42.

Davis, Jack. "Improving CIA Analytic Performance: Strategic Warning," *Sherman Kent Center for Intelligence Analysis* Occasional Papers 1, no. 1 (2002): 1–8.

Davis, Jack. "Strategic Warning: If Surprise Is Inevitable, What Role for Analysis?" *Sherman Kent Center for Analysis* Occasional Papers 2, no. 1 (2003): 1–16

Department of Defense. DoD Directive 3115.16: Defense Warning Network (Washington, DC, 2020). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/311516e.pdf?ver=2020-08-10-145143-097.

Director of Central Intelligence. "Memorandum for National Foreign Intelligence Board, Subject: Warning" (Washington, DC, July 17, 1992).

Director of Central Intelligence. "Task Force Report: Improving Intelligence Warning" (Washington, DC, May 29, 1992).

Director of Central Intelligence. Director of Central Intelligence Directive (DCID) No. 1/5: *National Intelligence Warning* (Washington, DC, May 23, 1979).

Gentry, John A. "Intelligence Failure Reframed," *Political Science Quarterly* 123, no. 2 (2008): 247–270.

Gentry, John A., and Joseph S. Gordon. *Strategic Warning Intelligence: History, Challenges, and Prospects* (Washington, DC: Georgetown University Press, 2019).

Grabo, Cynthia. *Handbook of Warning Intelligence: Complete and Declassified Edition* (Lanham, MD: Rowman and Littlefield, 2015).

H., Michael. "(U) A 'Feeling of Inadequacy': CIA Analyst of East Germany Looks Back to November 1989," *Studies in Intelligence* 63, no. 4 (2019): 1–5.

H., Michael. "(U) NIU Research Short: A Typology of Intelligence Surprise: A Framework for Enhanced Anticipation" (Washington DC: National Intelligence Press, December 3, 2019).

H., Michael. "Teaching 21st Century Warning Tradecraft," *Studies in Intelligence* 66, no. 1 (2022): 9–16.

Hamlet, Larry. "(U) NIU Research Short: Lessons from Outside the IC for Tracking Indicators" (Washington DC: National Intelligence Press, 2018).

Handel, Michael I. "The Yom Kippur War and the Inevitability of Surprise," *International Studies Quarterly 21*, no. 3 (1977): 461–502.

Hedley, John Hollister. "Learning From Intelligence Failure," *International Journal of Intelligence and Counterintelligence* 18, no. 3 (2005): 435–450.

Heilmeier, George H. "Guarding Against Tech Surprise," *Air University Review* 27, no. 6 (1976): 2–7.

Intelligence Warning Terminology (Washington, DC: Joint Military Intelligence College, 2001).

Joint Staff Directorate for Intelligence. *(U) Defense Warning Handbook* (2012).

Joint Staff Directorate for Intelligence. *(U) DoD Indications and Warning Systems Operations Manual,* J2M-0177-01-96, January 1997.

Jones, Reginald V. "Scientific Intelligence." *Journal of the Royal United Service Institution* 92 (1947): 352–60.

Lowenthal, Mark M. "Strategic Early Warning: Where Are We Now." *Journal of Intelligence and Analysis* 22, no. 2 (2015): 1–10.

Tessier, Scott. "(U) Improving Indications and Warning: Lessons from a Decade of Russian Intervention," *Studies in Intelligence* 61, no. 3 (2017): 1–17.

Vedantam, Shankar. "Warnings, Warnings Everywhere: Why We Sometimes Ignore Looming Disasters," Hidden Brain, Podcast Audio, January 20, 2020. https://www.npr.org/2020/01/17/797357603/the-cassandra-curse-why-we-heed-some-warnings-and-ignore-others.

Weinbaum, Courtney et al. "Perspectives and Opportunities in Intelligence for US Leaders" (Santa Monica, CA: RAND Corporation, 2018): 5–15.

Appendix B: Expert Consultation and NIU Workshop Questions

Questions for Expert Consultation Discussion

1. How would you describe your role or responsibility when it comes to warning?
   a. Probing/Follow Up 1: Would you consider yourself to be somebody who directly or indirectly provides warnings to policymakers or decisionmakers?

2. How would you define warning?
   a. Probing/Follow Up 1: Do you ever use the term strategic or tactical warning or other terms, and how do they differ from that general definition of warning?
   b. Probing/Follow Up 2: How does time play into your definitions of warning?
   c. Probing/Follow Up 3: Can you recall any episode when differences in opinion over warning definitions had consequences in terms of analysis, coming to a decision, or adopting a policy? Did the issue ever become resolved, and what was that resolution?

3. Do you consider warning to be a unique intelligence discipline or mission? And, if so, what makes it unique?
   a. Probing/Follow Up 1: Some authors or intelligence officers in the past have noted that analysts are ingesting information that can be used to support current intelligence or put in context for more strategic or warning applications. Is the process or mindset different for these tasks?
   b. Probing/Follow Up 2 (if they respond "no" to the main question): Would you say then that warning is an inherent element of intelligence?

4. From your perspective, what is required for warning analysis, warning intelligence, or warning in general to be considered successful?
   a. Probing/Follow Up: If a warning is delivered but not acted upon, would that be seen as a success still, a failure, or something else?
   b. Probing/Follow Up 2: Can you think of a specific example where you would say warning was successful or a failure, and what is it about the outcome that makes you classify it as such?

    c. Probing/Follow Up 3: Can you think of a contrasting example of an event that you could classify as a [success/failure], what was responsible for that outcome, and what makes the difference between success and failure?

5. Based on our conversation today, can you think of any issues, examples, subjects, or terms that seem important or have been especially relevant to your warning experiences?
6. Are there any other individuals, either in the IC or not, who might be good to talk with and interview as well?

Group Discussion Prompts for NIU Warning Workshop

1. When we discuss warning, what do we mean by "warning" and what falls under that umbrella? What is the intelligence enterprise's responsibility for warning?
2. What is the driving edge, or the innovative edge, of warning for the IC?
3. What drives your perspective on warning or the perspective of your organization?
4. What are the most significant challenges you believe the IC faces with regard to warning? This can include agency-specific challenges or broader issues.
5. What challenges and opportunities exist for the application of new, technical approaches—such as data science and quantitative analysis, machine learning, and artificial intelligence—to the IC's warning mission? How do you see the state of technical competency in this space?
6. What do intelligence officers (civilian and military), regardless of their career track, need to understand about the overall warning mission? What related topics should they be versed in? What are the terms they should be familiar with?

Appendix C: Listing of Unique Codes Organized by Subcategory

Guarding Against Surprise

Surprise

Primacy of "Surprise" and Its Effects

Strategic Surprise
Sudden Surprise
Implies Urgency
Association with Urgency
Suddenness
Surprise
Something Unexpected Always Happens
Degree of Surprise
Abrupt Transition/Dramatic Event
Tipping Point
Highly Compressed Timelines

Inevitability of Surprise/Failure

Perfection Is an Illusion
Flawed Expectations
Unrealistic Expectations
Inevitability of Surprise
Inevitability of Failure
Success to Failure Ratio
Paradox of Warning
Difficulty of Assessing Intent

Shock and Psychological Effect

Suddenness (overlap with current intel)
Psychological Effect of Surprise
Level of Shock Determines "Strategic Surprise"

Core Warning Mission

Lexicon

Warning
Tactical Warning (tactical as actionable)
Strategic Warning (things we do not yet know)
Sufficient Gravity To Put Nation at Risk
Warning Analysis (Def)
Intelligence Failure
Strategic Surprise
Unambiguous Warning
Emerging and Enduring
Anticipatory Intelligence
Operational Warning

Purposes of Warning

Avoid Damage, Not Avoid Surprise
Damage Limitation
Preparation Better Than Perfect Info
Warn in Advance of Indicators
Prevent and Disrupt Attacks
Understand the Landscape
Threat Landscape
Specialized Tradecraft
Prevent Surprise
Identify Threats and Opportunities
Develop Range of Options
Reduce Ambiguity

Achieving Analytic Success

Analytic Recommendations and Needs

Indicators
Chronology
Competing Hypotheses
Multiple Scenarios
Scenarios as Models
Authentic Devil's Advocates
Alternative Scenarios
Triggers and Signposts
Defined End States
Structured Analytic Techniques

Necessary Elements of Successful Warning

Analysis of Alternatives
Blue Sky Thinking (explore landscape)
"What If" Thinking
Nonlinear Thinking
Imagination
Seeing the Implications
Diversity of Views
Creativity

Lack of Perspective on Success

Study Success
How To Measure Success
Compare Success to Failure
Importance of Learning
Need To Integrate Social Science

Distinct Elements of Mission

The Nature of a Warning Mindset

Worst Case Scenario
Warning as a Mindset
Perspective of Surprise
Possibilities More Than Probabilities
Different Perspective/Minority View
Broader Context
Broader Time Horizons
Contrarian (Alternative Analysis)
Attitude
Vulnerability
Normal vs. Exceptional Thinking
Envelope of Possibilities
Future World of Potential
Future Orientation

Centrality of Mindset and Status Quo Preference

Mindsets
Disregard of Alternatives
Status Quo Bias
Need To Have Mindset of the Adversary
Seize and Freeze
Need for Cognitive Closure

Differentiation From Other Missions

Baseline and Anomalies
Anomaly Detection
Change Detection
Filter Signal From Noise
Discontinuities
Larger Context
Intent and Focus To Find Threats
Red Teams
Elevation of Minority Opinions

Communication for Effect

Nature of the Communication

Communication to Those Who Can Act

Communication to Decisionmakers (National or Other)
Multiple Links in Communication Process
Communication
Bespoke Communication
Tailored to a Specific Action

Timing of the Communication

Timing (Perfect, Too Early, Too Late)
Time Horizons
Timely Communication
Timeliness
Cry Wolf
Timely for Action
Threshold for Notification (Knowing When To Warn)
In Time To Act

Conditions for Communication

Phase Transition
Qualitative Change
Trend Continuity
Change in Analytic Line

Requirements for Communication

Clarity in Communication
Precise Language
Convey Accurately but Without Hype (contradicts persuasion)
Accuracy (+ necessary but not sufficient)
Explicit Warning
Balance Confidence and Accuracy
Tailored Production
They Must Know They Have Been Warned
Balance Urgency With Over-alarming

Responses: Action or Decision

Imperative To Convince

Persuasion
Convincing
Make Warning Stick in the Minds
Make it Stick
Must Be Distinct
Credibility To Motivate
Sufficient Information To Allow Action
Warning as Marketing

A Requirement for Action

Need To Act for Warning To Be Effective
Action To Address Tangible Issue
Theory of Preventive Action
Tying Success to Action
Needs To Trigger an Action
Competing With Current Analysis
Contrast With Current Intelligence

Prompting Informed Decisions

Decision Space
Decision Advantage
Interaction of Intel and Decisionmaking
Success Prompts a Decision To Make
Decision Can Be Not To Act
Opportunities To Act
Acceptable Level of Readiness
Success in Drawing Attention
Decision Support
Understanding Consequences

Warning-Response Process

Response to Warning
Must Elicit Response
Intel-Warning-Response
Warning-Response Process

Intel/Policy Relationship

Importance of Relationship

Collaborative Between Policy and Analysis
Red-Blue
Impact of Trust in Relationship
Personal Relationship
Receptivity
Increase Receptivity to Warning
Danger of Repeated Warning
Daily Briefer Relationship and Trust
Trust and Credibility
Intel-Policy Relationship
Producer-Consumer Interactions

Tension in the Relationship

Analysis Decision Separation
Separation of Intel and Policy
Intel as a Scapegoat
Government vs. Intelligence Responsibility
"State Failure"
Intel as One of Many Inputs
Dissent
Opportunities Without Advocating

Nature/Role of the Customer

Assessments Run Counter to Policy Preferences
Educated Customers
Role of Consumers in Failure
Decisionmakers as Analysts
Resistant Customers
Policymaker Prioritizations
Opportunity Costs of Being Wrong
Costs of Preparation

Intelligence Needs for Success

Opportunity Analysis
Need To Understand the Policy Space
Personal Relationship w/Customer
Know What Decisionmakers Need
Need To Understand Blue Policy Issues with Specificity
Intel Must Know Who and How To Warn
Understand the Consumer
Solutions and not Just Problems
Lean Forward (confidence vs. time)
Understand Consumer Process
Include Risk Assessment

The Threat Landscape

Multiplicity of Threats

Risk Triaging and Prioritizing
Triage Among Threats
Triage of Warning
Multiplicity of Threats
Need To Keep Threats Finite
Triaging and Ranking Threats
Prioritization (rapid change of past prioritization)
Worst Case Planning Impossible (limited resources)
Calibrate Threats
Diverse Threats
Identify-Categorize-Understand
Changing Nature of Threats

Timing of the Threat

Timeline (e.g., not to exceed six months)
Prediction of Timing Is Folly
Danger in Timing Pre-judgment
Assessing Timing Most Difficult Task
Creep of Normalcy
Relationship to Time
Routinization of Tension
Alert Fatigue
Linear vs. Nonlinear Threats

Conceptualizing the Threat

Probability vs. Imminence
Probability vs. Impact
Capability vs. Intentions
Assessing Intentions

The Operational Environment

Uncertainty and Ambiguity

Signal and Noise Paradox

Ambiguity
Ambiguity Barrier

Ambiguity Enables Biases
Hedging
Hedging Against Uncertainty
Deception
Uncertainty (Nature of the World)

Biases That Inhibit Successful Warning

Paradox of Expertise
Biases
Continuity Bias
Hindsight Bias
Optimism Bias
Confirmation Bias
Defense Planning Bias
"Boiling Frog" Problem
Unchallenged Assumptions
Poverty of Imagination
Failure To Think of the Unthinkable
Mirror Image
Straight Line Extrapolations
Overcoming Mindsets (Holding to Beliefs/ Need To Unfreeze Decisionmakers)
Lack of Cultural Understanding

Complexity

Complexity in the International Environment

Complex Environment
Ignorance of Complexity
Complexity

Organize To Execute

Structural Challenges (Organization and Procedure)

Centralized vs. EAAWA
Atrophy of Reforms
Organization Changes
Gaps and Seams in Analysis
Bystander Effect
Ritualized Mission
Trappings of Doctrine
Tyranny of the Now or Urgent
Current Intel Focus
Difficulty of Democracy
Low NIPF Rankings
Differing National Priorities
Need for Specialization
Methodology Specialization
Compartmented Data
Process
Sequence
Structure of Mission
"Manage" the Mission
Expertise vs. Indicators
Pressure for Speed, Decisiveness

Sub-Disciplines/Application Areas

Military Actions
Political Instability
Challenges of Cyber (deniability, anonymity)
Space
Counterterrorism
Technical/Technology Surprise

Endnotes

1. Richard A. Clarke and R. P. Eddy, *Warnings: Finding Cassandras to Stop Catastrophes* (New York: Harper Collins, 2017): 167–95.
2. Department of Defense, DoD Directive 3115.16: The Defense Warning Network (DWN), Change 2 (Washington, DC: 2020).
3. John A. Gentry and Joseph S. Gordon, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Washington, DC: Georgetown University Press, 2019): 56–58.
4. Kathy Charmaz, *Constructing Grounded Theory,* 2nd ed. (London: Sage, 2014): 1–20.
5. John A. Gentry, "Intelligence Failure Reframed," *Political Science Quarterly* 123, no. 2 (2008): 247–70.
6. Daniel F. Landers, "The Defense Warning System," *Defense Intelligence Journal* 3 (1994): 21–32.
7. Erik Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013): 6–24.
8. George H. Heilmeier, "Guarding Against Tech Surprise," *Air University Review* 27, no. 6 (1976): 2–7.
9. DoD Joint Staff Directorate for Intelligence (J-2); 2017; (U) Defense Warning Network (DWN) Handbook*,* 4th ed.; Classification of extracted material is U.
10. Christoph Meyer et al., *Warning About War* (Cambridge, UK: Cambridge University Press, 2020): 22.
11. Courtney Weinbaum et al., *Perspectives and Opportunities in Intelligence for US Leaders* (Santa Monica: RAND Corporation, 2018): 5–15.
12. National Intelligence University, "*Exploring the Foundations and Frontiers of Warning*" (Professional Workshop, Intelligence Community Campus-Bethesda, May 11, 2023).
13. Jordan Ellenberg, *How Not To Be Wrong: The Power of Mathematical Thinking* (New York: Penguin Press, 2014): 261–66.
14. Dahl, *Intelligence and Surprise Attack,* 175–84.
15. Uri Bar-Joseph and Rose McDermott*, Intelligence Success and Failure: The Human Factor* (New York: Oxford University Press, 2017): 235–40.
16. Meyer et al., *Warning About War,* 12–20.
17. Cynthia Grabo, *Handbook of Warning Intelligence: Complete and Declassified Edition* (Lanham, MD: Rowman and Littlefield, 2015): 1–8.
18. Gentry and Gordon, *Strategic Warning Intelligence,* 1–7.
19. Joint Chiefs of Staff, Joint Publication 2-0 (JP 2-0): Joint Intelligence (Washington, DC, May 26, 2022).
20. Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Thousand Oaks, CA: CQ Press, 2017), 20–27.
21. Grabo, *Handbook of Warning Intelligence,* 15–17.
22. Euan G. Davis, "A Watchman for All Seasons," *Studies in Intelligence* 13, no. 2 (1969): 37–42.
23. Mark M. Lowenthal, "Strategic Early Warning: Where Are We Now," *Journal of Intelligence and Analysis*, no. 2 (2015): 1–10.
24. Gentry, "Intelligence Failure Reframed," 247–70.

25. Gentry and Gordon, *Strategic Warning Intelligence*, 12.
26. John W. Bodnar, *Warning Analysis for the Information Age: Rethinking the Intelligence Process.* (Washington, DC: Joint Military Intelligence College, 2003), 1.
27. Gentry and Gordon, *Strategic Warning Intelligence,* 11–23.
28. Office of the Director of National Intelligence (ODNI), National Intelligence Strategy (Washington, DC, 2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.
29. J. Eli Margolis, "Rethinking Analytic Disciplines, Reordering the Profession," *Studies in Intelligence* 64, no. 4 (2020): 29-41.
30. ODNI, National Intelligence Strategy.
31. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook*,* 3rd ed.; 2014; Classification of extracted material is U.
32. John M. Schmidt, "Intelligence, Strategic Warning, and Foresight: Completing the Package for Decision-Makers," *Journal of Intelligence and Analysis*, no. 2 (2015): 11–29.
33. Gentry and Gordon, *Strategic Warning Intelligence,* 14.
34. Josh Kerbel, "The US Talks a Lot About Strategic Complexity. Too Bad It's Mostly Just Talk," *Defense One,* March 9, 2021.
35. Josh Kerbel, "Coming to Terms with Anticipatory Intelligence," *War on the Rocks,* August 13, 2019, https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/.
36. Kerbel, "Coming to Terms."
37. Gentry and Gordon, *Strategic Warning Intelligence,* 153–54.
38. Grabo, *Handbook of Warning Intelligence,* 20.
39. Michael H., "(U) A 'Feeling of Inadequacy': CIA Analyst of East Germany Looks Back to November 1989," *Studies in Intelligence* 63, no. 4; 1–5; 2019; Classification of extracted material is U.
40. Davis, "A Watchman for All Seasons," 37–42.
41. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
42. DOD J-2; (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
43. Director of Central Intelligence (DCI), Director of Central Intelligence Directive (DCID) No. 1/5: *National Intelligence Warning* (Washington, DC, May 23, 1979).
44. Keith Clark, "On Warning," *Studies in Intelligence* 9, no. 1 (1965): 15–21.
45. Michael H., "(U) A 'Feeling of Inadequacy': CIA Analyst of East Germany Looks Back to November 1989," *Studies in Intelligence* 63, no. 4 1–5; 2019; Classification of extracted information is U.
46. Gentry and Gordon, *Strategic Warning Intelligence*, 227.
47. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
48. DCI, "Task Force Report: Improving Intelligence Warning," May 29, 1992.
49. Grabo, *Handbook of Warning Intelligence,* 25–26.
50. Clark, "On Warning," 15–21.
51. Gentry, "Intelligence Failure Reframed," 247–70.
52. Joint Military Intelligence College, *Intelligence Warning Terminology* (Washington, DC: Joint Military Intelligence College, 2001): 24.
53. Meyer et al., *Warning About War,* 1–19.
54. Dahl, *Intelligence and Surprise Attack,* 6–24.

55. Clarke and Eddy, *Warnings,* 168–69.
56. Clarke and Eddy. *Warnings,* 351–67.
57. Michele Wucker, *The Gray Rhino: How To Recognize and Act on the Obvious Dangers We Ignore* (New York: St. Martin's Press, 2016): 1–27.
58. Jack Davis, "Strategic Warning: If Surprise Is Inevitable, What Role for Analysis," *Sherman Kent Center for Analysis Occasional Papers* 2, no. 1 (2003): 1–16.
59. Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (1978): 61–89.
60. Gentry, "Intelligence Failure Reframed," 247–70.
61. Erik Dahl, *The COVID-19 Intelligence Failure: Why Warning Was Not Enough* (Washington, DC: Georgetown University Press, 2023): 86.
62. Roger George and James Bruce, *Analyzing Intelligence: National Security Practitioners' Perspectives, 2nd ed.* (Washington DC: Georgetown University Press, 2014): 366, accessed March 20, 2023. ProQuest Ebook Central.
63. Grabo, *Handbook of Warning Intelligence,* 14.
64. DCI, DCID No. 1/5: *National Intelligence Warning*.
65. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 2012; Classification of extracted material is U.
66. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted material is U.
67. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
68. DOD Joint Staff Directorate for Intelligence (J-2); (U) DoD Indications and Warning Systems Operations Manual; J2M-0177-01-96; January 1997; Classification of extracted material is U.
69. DOD Directive 3115.16: DWN, Change 2.
70. Joint Chiefs of Staff, JP 2-0: Joint Intelligence.
71. Meyer et al., *Warning About War,* 6.
72. Joint Chiefs of Staff, JP 2-0: Joint Intelligence.
73. Joint Military Intelligence College, *Intelligence Warning Terminology,* 38.
74. Gentry and Gordon, *Strategic Warning Intelligence,* 1.
75. Davis, "A Watchman for All Seasons," 37–42.
76. DCI, DCID No. 1/5: *National Intelligence Warning*.
77. Joint Chiefs of Staff, JP 1-02: *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC, October 17, 2007).
78. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed; 2017; Classification of extracted information is U.
79. Joint Military Intelligence College, *Intelligence Warning Terminology,* 35.
80. Bar-Joseph and McDermott, *Intelligence Success and Failure,* 11.
81. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted information is U.
82. Gentry and Gordon, *Strategic Warning Intelligence,* 12.
83. Lowenthal, "Strategic Early Warning," 1–10.
84. Bodnar, *Warning Analysis for the Information Age,* 1.
85. DoD Directive 3115.16: DWN, Change 2.
86. Joint Military Intelligence College, *Intelligence Warning Terminology,* 28.

87. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

88. Bodnar, *Warning Analysis for the Information Age,* 1.

89. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

90. Grabo, *Handbook of Warning Intelligence,* 175–89.

91. Joint Military Intelligence College, *Intelligence Warning Terminology,* 29.

92. DOD; Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted material is U.

93. DOD; Joint Staff Directorate for Intelligence (J-2); (U) DoD Indications and Warning Systems Operations Manual; Classification of extracted material is U.

94. CIA; CIA-DA-2016-02997; January 26, 2017; (U) The Fragile Chain of Warning; Classification of extracted material is U.

95. Betts, "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly* 95, no. 4 (1980–1981): 551–72.

96. Gentry, "Intelligence Failure Reframed," 247–70.

97. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted material is U.

98. SCITEK, *(U) Indications and Warning Intelligence* (Washington, DC: Defense Intelligence School, 1974): 1–6. Classification of cited portion is UNCLASSIFIED.

99. DOD Inspector General (IG); DODIG-2020-055; January 30, 2020; "(U) Evaluation of US European Command's Warning Intelligence Capabilities," (Redacted); Classification of extracted material is U. https://www.oversight.gov/report/dod/evaluation-us-european-commands-warning-intelligence-capabilities.

100. Gentry and Gordon, *Strategic Warning Intelligence,* 111.

101. Grabo, *Handbook of Warning Intelligence,* 175.

102. DCI, "Task Force Report: Improving Intelligence Warning."

103. Grabo, *Handbook of Warning Intelligence,* 41–47.

104. Grabo, *Handbook of Warning Intelligence,* 41–47.

105. Michael Handel, "The Yom Kippur War and the Inevitability of Surprise," *International Studies Quarterly* 21, no 3 (1977): 461–502.

106. Lowenthal, "Strategic Early Warning," 1–10.

107. Kerbel, "Coming to Terms."

108. Gentry and Gordon, *Strategic Warning Intelligence,* 55–64.

109. John Gentry and Joseph Gordon, "US Strategic Warning Intelligence: Situation and Prospects," *International Journal of Intelligence and Counterintelligence* 31 (2018): 19–53.

110. Landers, "The Defense Warning System," 21–32.

111. DOD Joint Staff Directorate for Intelligence (J-2); (U) DoD Indications and Warning Systems Operations Manual; Classification of extracted material is U.

112. DOD Joint Staff Directorate for Intelligence (J-2); (U) Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

113. DCI, "Memorandum For National Foreign Intelligence Board, Subject: Warning," July 17, 1992.

114. DoD Directive 3115.16: DWN, Change 2.

115. Reginald V. Jones, "Scientific Intelligence," *Journal of the Royal United Service Institution* 92 (1947): 352–60.

116. Jones, "Scientific Intelligence," 352–60.

117. Gentry and Gordon, *Strategic Warning Intelligence,* 43.
118. Davis, "A Watchman for All Seasons," 37–42.
119. Joint Military Intelligence College, *Intelligence Warning Terminology,* 12.
120. Lowenthal, "Strategic Early Warning," 1–10.
121. Clark, "On Warning," 15–21.
122. Lowenthal, "Strategic Early Warning," 1–10.
123. Davis, "A Watchman for All Seasons," 37–42.
124. Joint Military Intelligence College, *Intelligence Warning Terminology,* 12.
125. Joint Chiefs of Staff, JP 2-0: Joint Intelligence.
126. Grabo, *Handbook of Warning Intelligence,* 60–65.
127. Gentry and Gordon, *Strategic Warning Intelligence,* 131–47.
128. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
129. DOD J-2, (U) DoD Indications and Warning Systems Operations Manual; Classification of extracted material is U.
130. DOD J-2, (U) DoD Indications and Warning Systems Operations Manual; Classification of extracted material is U.
131. Randolph Pherson and John Pyrik, *Analyst's Guide to Indicators,* (Reston, VA: Pherson Associates LLC, 2017).
132. Gentry and Gordon, *Strategic Warning Intelligence,* 133.
133. DOD J-2; Defense Warning Network (DWN) Handbook, 3rd ed.; 2014; Classification of extracted material is U.
134. Grabo, *Handbook of Warning Intelligence,* 77–90.
135. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
136. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.
137. Davis, "Strategic Warning: If Surprise Is Inevitable," 1–16.
138. John Hughes-Wilson, *Military Intelligence Blunders and Cover-Ups* (New York: Carroll and Graf Publishers, 2004): 1–10.
139. Rebecca Wholstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962): 1–5.
140. National Commission on Terrorist Attacks, *The 9/11 Commission Report* (New York: WW Norton, 2004): 408.
141. Dahl, *Intelligence and Surprise Attack,* 68–80.
142. Bar-Joseph and McDermott, *Intelligence Success and Failure,* 9–26.
143. Handel, "The Yom Kippur War," 461–502.
144. Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Simon & Schuster, 1990): 5–20.
145. Dahl, *Intelligence and Surprise Attack,* 6–28.
146. Abraham Ben-Zvi, "The Study of Surprise Attacks," *The British Journal of International Studies* 5, no. 2. (1979): 129–49.
147. Bar-Joseph and McDermott, *Intelligence Success and Failure,* 48–52.
148. Betts, "Analysis, War, and Decision," 61–89.
149. Michael Handel, "Intelligence and the Problem of Strategic Surprise," *Journal of Strategic Studies* 7, no 3. (1984).
150. Robert Jervis, "Hypotheses on Misperception," *World Politics* 20, no. 3 (1968): 454–79.
151. Davis, "Strategic Warning: If Surprise Is Inevitable," 1–16.
152. Betts, "Surprise Despite Warning," 551–72.
153. Gentry, "Intelligence Failure Reframed," 247–70.
154. Bar-Joseph and McDermott, *Intelligence Success and Failure,* 48–52.
155. Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988): 37–55.
156. Ariel Levite, *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987): 1.
157. Michael H., "(U) A Typology of Intelligence Surprise: A Framework for Enhanced Anticipation," *Research Short,* National Intelligence Press, December 3, 2019.

158. Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007): 3–6.
159. Wucker, *The Gray Rhino,* 1–26.
160. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus, and Giroux, 2011): 19–30.
161. Richards J. Heuer, *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999): xiii.
162. John A. Gentry, "Cyber Intelligence: Strategic Warning is Possible," *International Journal of Intelligence and Counterintelligence* 36, no. 3 (2023): 1–26.
163. Michael H., "(U) A Typology of Intelligence Surprise."
164. Kerbel, "Coming to Terms."
165. Maike Vollstedt and Sebastian Rezat, "An Introduction to Grounded Theory with a Special Focus on Axial Coding and the Coding Paradigm," in *Compendium for Early Career Researchers in Mathematics Education,* Gabriele Kaiser and Norma Presmeg, eds. (Switzerland: Springer Open, 2019).
166. Charmaz, *Constructing Grounded Theory,* 1–20.
167. Charmaz, *Constructing Grounded Theory,* 1–20.
168. Anne O'Connor et al., "An Exploration of Key Issues in the Debate Between Classic and Constructivist Grounded Theory," *The Grounded Theory Review* 17, Issue 1 (2018).
169. O'Connor et al., "An Exploration of Key Issues."
170. Grabo, *Handbook of Warning Intelligence,* 14.
171. Charmaz, *Constructing Grounded Theory,* 22–54.
172. J. S. Chen, "Harm Reduction Policy in Taiwan: Toward a Comprehensive Understanding of Its Making and Effects," *Harm Reduction Journal* 13, no. 11 (2016).
173. Helen Hardman, "The Validity of a Grounded Theory Approach to Research on Democratization," *Qualitative Research* 13, no. 6 (2012): 635–49.
174. Glenn A. Bowen. *"Social Funds as a Strategy for Poverty Reduction in Jamaica: An Exploratory Study*," Florida International University Dissertation, A 65/04 (2003).
175. Glenn A. Bowen, "Local-Level Stakeholder Collaboration: A Substantive Theory of Community-Driven Development," *Journal of the Community Development Society* 36, no. 2 (2005): 73–88.
176. Glenn A. Bowen, "Document Analysis as a Qualitative Research Method," *Qualitative Research Journal* 9, no. 2 (2009): 27–40.
177. Nicholas Ralph et al., "Contextual Positioning: Using Documents as Extant Data in Grounded Theory Research," *SAGE Open Journal* (July–September 2014): 1–7.
178. Vollstedt and Rezat, "An Introduction to Grounded Theory."
179. Ralph et al., "Contextual Positioning," 1–7.
180. Charmaz, *Constructing Grounded Theory,* 109–150.
181. Ralph et al., "Contextual Positioning," 1–7.
182. Heuer, *The Psychology of Intelligence Analysis,* 23–24.
183. Kahneman, *Thinking, Fast and Slow,* 19–30.
184. Levite, *Intelligence and Strategic Surprises,* 1.
185. DoD*,* Recorded Comments of CJCS Colin Powell to Joint Staff Warning Conference, Washington, DC, CAC632 Course Materials, 5-minute segment (circa 1992).
186. Scott Tessier, "(U) Improving Indications and Warning: Lessons from a Decade of Russian Intervention," *Studies in Intelligence* 61, no. 3 (2017): 1–17. Classification of extracted material is U.
187. Interview with Senior-Level Intelligence Official by Johnathan Proctor, Tyson's Corner, VA, March 2023.
188. George and Bruce, *Analyzing Intelligence,* 366.

189. Dahl, *Intelligence and Surprise Attack*, 2.

190. Adrian Wolfberg, "The President's Daily Brief: Managing the Relationship Between Intelligence and the Policymaker," *Political Science Quarterly* 132, no. 2.

191. Robert Kaplan and Anette Mikes, "Managing Risks: A New Framework," *Harvard Business Review* 90, no.6 (June 2012).

192. DCI, DCID No. 1/5: *National Intelligence Warning*.

193. Gentry and Gordon, *Strategic Warning Intelligence,* 14.

194. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

195. Noel Buckner and Rob Whittlesey, "In the Path of a Killer Volcano," Public Broadcasting Service, *NOVA,* Season 20, Episode 5 (1993).

196. Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010), 15–33.

197. Wholstetter, *Pearl Harbor,* 1–5.

198. Handel, "Intelligence and the Problem of Strategic Surprise."

199. Handel, "Intelligence and the Problem of Strategic Surprise."

200. Larry Hamlet, "(U) Lessons From Outside the IC for Tracking Indicators," *Research Short,* National Intelligence Press, 2018, Classification of extracted material is U.

201. Clark, "On Warning," *Studies in Intelligence* 9, no. 1 (1965): 15–21.

202. Department of Justice, "National Commission on Forensic Science: Views of the Commission on Inconsistent Terminology," April 30, 2015. https://www.justice.gov/archives/ncfs/page/file/1004446/dl.

203. Josh Kerbel, "Stop Using 'Strategic' To Mean Everything Under the Sun," *Defense One,* October 31, 2016. https://www.defenseone.com/ideas/2016/10/stop-using-strategic-mean-everything-under-sun/132790/.

204. Joint Chiefs of Staff, JP 2.0: Joint Intelligence. https://jdeis.js.mil/jdeis/index.jsp?pindex=4.

205. DoD Directive 3115.16: DWN, Change 2.

206. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

207. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

208. Lowenthal, "Strategic Early Warning," 1–10.

209. Gentry and Gordon, *Strategic Warning Intelligence,* 12.

210. Gentry, "Cyber Intelligence," 2–3.

211. Gentry and Gordon, *Strategic Warning Intelligence,* 12.

212. DCI, DCID No. 1/5: *National Intelligence Warning*.

213. Dahl, *Intelligence and Surprise Attack,* 22.

214. Gentry and Gordon, *Strategic Warning Intelligence,* 15.

215. DOD J-2; Defense Warning Network (DWN) Handbook, 4th ed.; 2017; Classification of extracted material is U.

216. Shankar Vedantam et al., "Warnings, Warnings Everywhere: Why We Sometimes Ignore Looming Disasters," *Hidden Brain,* Podcast Audio, January 20, 2020. https://www.npr.org/2020/01/17/797357603/the-cassandra-curse-why-we-heed-some-warnings-and-ignore-others.

217. Michael H., "(U) A Typology of Intelligence Surprise."

218. Clarke and Eddy, *Warnings,* 180.

219. Bar-Joseph and McDermott*, Intelligence Success and Failure,* 94–95.

220. Philip Tetlock and Dan Gardner*, Superforecasting: The Art and Science of Prediction* (New York: Broadway Books, 2015): 103.

221. Peter Trubowitz and Kohei Watanabe "The Geopolitical Threat Index: A Text-Based Computational Approach to Identifying Foreign Threats," *International Studies Quarterly*, Issue 3 (September 2021): 1–14.

222. Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997): 34–60.

223. Thomas Schelling, *Micromotives and Macrobehaviors* (New York: Norton and Company, 1978): 135–166.

224. DOD IG, "(U) Evaluation of US European Command's Warning Intelligence Capabilities" (Redacted). https://www.oversight.gov/report/dod/evaluation-us-european-commands-warning-intelligence-capabilities.

225. Josh Kerbel, Lecture Presented to NIU Course CAC631, March 2022.

226. Meyer et al., *Warning About War,* 78.

227. Vedantam, "Warnings, Warnings Everywhere."

228. Wolfberg, "The President's Daily Brief."

229. Clarke and Eddy, *Warnings,* 356–58.

230. Meyer et al., *Warning About War,* 1–20.

231. Grabo, *Handbook of Warning Intelligence,* 103–107.

232. Gentry and Gordon, *Strategic Warning Intelligence,* 219.

233. Heuer, *The Psychology of Intelligence Analysis,* 23–24.

234. Carol Dweck, Mindset: *The New Psychology of Success* (New York: Penguin Random House, 2016): 57–70.

235. Gentry and Gordon, *Strategic Warning Intelligence,* 215–30.

236. Gentry and Gordon, *Strategic Warning Intelligence,* 215–30.

237. Clarke and Eddy, *Warnings,* 355–356.

238. Josh Kerbel, "The Metaphor Is the Message: Reconsidering Word Use for Today's Security Environment," *Research Short,* National Intelligence Press, December 5, 2017.

239. Josh Kerbel, "By Calling It a 'Cold War' We Risk Containing Ourselves," *The Hill,* October 3, 2022. https://thehill.com/opinion/national-security/3667479-by-calling-it-a-cold-war-we-risk-containing-ourselves/.