NATIONAL INTELLIGENCE UNIVERSITY

Ann Caracristi Institute For Intelligence Research

What this is:

This report is the product of academic research. As the IC's university, NIU is uniquely positioned to use academic approaches to research—and report on—subjects of interest to the community.

What this is not:

This is not finished intelligence. The opinions expressed in this report are solely the author's and not those of National Intelligence University, or any other US Government agency.

RESEARCH SHORT

CATALYST Designed to spark positive conversations on the future of the IC

March 14, 2024

IMAGE FROM SHUTTERSTOCK

Integrating GenAI and Strategic Foresight for 21st Century National Security

LtCol Jake Sotiriadis, Ph.D.

Today's political leaders are using military force as a go-to solution for geopolitical disputes in Ukraine, Gaza, and beyond. This assertiveness is not confined to isolated regions; it is an emergent global phenomenon. Victory in these and future conflicts requires pivoting to a foresight-based approach that informs strategies rooted in a deep understanding of complex global dynamics. Building a generative-artificial intelligence (GenAI)-powered "cognitive operating system" to navigate uncertainty can harness GenAI's ability to synthesize vast arrays of data into coherent, actionable insights. Integrating GenAI with strategic foresight will bolster the US national security ecosystem's capacity to think, act, and adapt in an unpredictable, ever-changing global landscape.

21st Century Global Complexity and Perpetual Conflict

The violence ravaging the Middle East and Ukraine in 2024 highlights the inadequacy of linear thinking in a global landscape marred by destabilizing factors that transcend security politics. These multiplying flashpoints underscore a world in "polycrisis"—one beset by converging economic, geopolitical, and technological disruptions that confound traditional security paradigms.[1] Yet the US intelligence and military communities persist in applying outdated mental models to these new challenges, which transcend traditional statecraft. The national security ecosystem needs a fundamental upgrade to its strategic analysis and foresight capabilities to better anticipate change in this complex world. Only by revolutionizing how we perceive, act, and adapt can we forge a comprehensive strategic synthesis—that applies not just to today's challenges but also to the unforeseen trials of tomorrow. It demands leaders who think in systems, wield technology with foresight, and navigate uncertainty with vision.

Hybrid threats that blend digital misinformation with physical conflict are testing the national security enterprise's readiness. Less than a year ago—in May 2023—AI-generated images of a nonexistent explosion at the Pentagon spread like wildfire across the Internet.[2] Their impact quickly jumped beyond the immediate sphere of national security to the financial sector when the stock market opened and the Standard & Poor's 500 index immediately (if modestly) fell.[3] This complex interplay between digital misinformation, national security, and the economy should warn us that a single move—real or fabricated—can have instant cascading effects across multiple domains.

Indeed, complexity remains the *only* constant, with "wicked problems"[*] defying the boundaries of traditional, clearly defined solutions.[4] Such complexity precludes straightforward answers or one-size-fits-all strategies that can untangle the dense web of emergent phenomena. Simply wielding the most superior technology—often the default solution for the United States—cannot guarantee success without a strategic framework that accounts for the interdependence of global phenomena.

A GenAI-Powered Cognitive Operating System for the 21st Century

In an era when the volume and speed of information exceeds human ability to comprehend it, national security demands more than smartphone-like applications that offer instant solutions. More fundamentally, our efforts must begin with the true "hardware" of our human capital—the minds of our people. In computer science, an operating system is a program that acts as an interface between the computer user and computer hardware and controls the execution of programs.[5] Just as a computer's operating system serves as a critical interface between the user and the machine's hardware, so, too, must we develop a cognitive operating system within national security contexts. This system's "circuits" are the mental processes and frameworks

[*] Wicked problems are complex social or cultural problems with an unknown number of potential solutions. Horst Ritiel, Milvin Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4 (1973): 155–169.

that intelligence and military personnel use to navigate complexity, critically evaluate information, challenge preconceived notions, and identify inherent biases. The system is "programmed" to reject superficial analyses in favor of profound comprehension, mirroring the way a computer runs diagnostics to detect and mitigate vulnerabilities.

In a national security context, such a system ensures familiarity with foresight-based frameworks that emphasize adaptability and a tolerance for uncertainty.[6] By leveraging these tools, individuals and organizations can better anticipate shifts, prepare for unanticipated outcomes, and navigate the ambiguity that defines the current era.[7] The outcome can be a set of well-considered, strategic decisions that enhance national security and address the multifaceted challenges posed by a given challenge or crisis.

Today, we are on the cusp of a transformative shift with the advent of GenAI tools.[8] Advanced algorithms can process and analyze vast quantities of data faster than any human, identifying patterns and connections that might otherwise go unnoticed. Relying on automation alone, however, overlooks a critical aspect of "sensemaking" defined as the need for *contextualized* knowledge. Our ability to understand the story comes from deep knowledge of cultural, historical, geopolitical, and human factors that algorithms cannot yet fully grasp. Context matters. The same event can have different implications in different parts of the world, and cultural and historical nuances often shape these interpretations. Human experts can put things into context, something that automated systems are far from replicating.[9]

> Sensemaking is not just about connecting dots; it is about understanding the story those dots tell.

The ideal balance in the cognitive operating system is to harness both the power of GenAI, including advanced language models, and human-inspired context to enhance strategic foresight of risk and opportunity. This system rests on three pillars:

1. Seeing the interconnectivity of events.
2. Challenging the status quo.
3. Embracing analytic complexity in decisionmaking.

This approach underscores the importance of human cognitive capabilities in managing and responding to global security challenges, where computational tools aid—but do not replace—the nuanced understanding and critical thinking skills of human actors. Military and intelligence personnel will need to be able to connect disparate pieces of information, identify patterns and anomalies, and craft potential future scenarios *in tandem* with GenAI tools.[10]

GenAI tools are instrumental to this partnership in the following ways:

- Discerning foundational scenarios by identifying trends in the data to establish a robust starting point for planning.
- Applying predictive analytics to extensive databases to craft scenarios in line with evolving trends that enhance the accuracy and vision of planning efforts.

- Contributing novel ideas and potential strategies, adding depth to strategic thinking.
- Simplifying the integration of multiple scenarios to streamline the planning and risk-assessment process.
- Offering critical analysis of possible strategies for handling potential scenarios to identify the most effective options for organizational resilience.[11]

The Pillars of a GenAI-Powered Cognitive Operating System

Pillar 1: Seeing the Interconnectivity of Events

Recognizing the intricate and often subtle links among occurrences in different domains or regions is fundamental to developing a broad and interconnected view of global events. This interconnectivity requires intelligence analysts and strategists to consider a broader range of variables and potential consequences when assessing threats and developing opportunities to counter them. Today's interconnected reality provides endless examples of how a seemingly insignificant event in a remote location or domain can quickly trigger a major crisis: a rogue algorithm in a stock-trading system triggers a financial meltdown; a cyber attack on a smart grid plunges cities and towns into darkness; or a *faux pas* on social media escalates into a full-blown conflict.

This pillar is pivotal in spotting cause-and-effect patterns that span disparate domains and geographies. Exploiting this capability requires a multidisciplinary approach to problem-solving and decisionmaking that considers historical precedents, current events, and deeply contextualized projections. This perspective aids in identifying nonobvious relationships and dependencies that might not be quickly apparent but are crucial for a complete understanding of the situation at hand.

Pillar 2: Challenging the Status Quo

A cultural shift is needed within the national security enterprise to foster an environment where questioning and creative thinking are encouraged. It portends a rigorous reassessment of entrenched strategies, doctrines, and tactics, paving the way for groundbreaking approaches that may starkly diverge from conventional military and intelligence paradigms. Embracing such innovation requires more than an openness to change; it demands an institutional transformation that places a premium on disruptive thinking. The intelligence and military communities must cultivate a climate that actively encourages exploring unorthodox ideas and constructive dissent to bring about a strategic evolution. This environment should reward adaptability, promote continuous learning, and encourage collaboration across diverse disciplines; harnessing insights from technology, psychology, and other fields to enrich strategic thought processes.

The national security enterprise has taken steps to create a military "Internet of Things." Initiatives, such as the Joint Warfighting Concept and Joint All-Domain Command and Control,

are commendable efforts to integrate digital connectivity into military operations.[12] This digital makeover aims to enhance the US military's ability to communicate and make swift decisions in conflict scenarios, especially against peer adversaries. Big data and AI are at the forefront of this transformation, designed to synchronize sensors and shooters across multiple domains.[13] This solution, however, like so many before it, is platform-centric—not human-centric.

To its credit, the Joint Staff, in "Developing Today's Joint Officers for Tomorrow's Ways of War" highlights an urgent need to reform the training and development of military personnel.[14] Notably, the document introduces the concept of intellectual overmatch, which emphasizes the need for superior cognitive capabilities in future conflicts.[15] But, talk is cheap. The real challenge lies in evolving this concept from paper to practice—devising actionable steps and measurable criteria to cultivate and deploy these advanced cognitive skills in global conflict and security operations. For now, the US military and IC are betting on big tech to deliver the goods, but that only addresses half of this equation. Upgrading digital platforms, while necessary, is far from sufficient because our *current* cognitive operating system—characterized by highly structured, linear thinking—is ill-suited to the shifting nature of modern conflict.

Pillar 3: Embracing Analytic Complexity in Decisionmaking

Understanding complexity theory—which suggests that diverse, interconnected elements can lead to unpredictable behavior and emergent phenomena in large systems[17]—is critical because national security is no longer about linear cause-and-effect scenarios. Rather, it involves multifaceted threats that require deep analytical insight to identify patterns and anticipate changes. These threats can rapidly evolve and adapt, reflecting the dynamic interplay of myriad factors—from geopolitical shifts to technological advancements. Unlike the first pillar, which focuses on seeing connections, this pillar delves into the complexities of systems where countless interrelated factors lead to unpredictable outcomes. Imagine a cyber security breach where the ripple effect impacts not just digital infrastructure but also political relations and market stability. Embracing analytic complexity trains intelligence analysts to decode intricate scenarios, in which multifaceted threats evolve rapidly and demand deep understanding to foresee shifts and patterns in a world where change is the only constant.

> Nearly 25 years ago, the world braced for a crisis born from underestimating a system's complexity. The Y2K bug at the turn of the century held the potential for global upheaval, rooted not in advancing armies or the ambitions of dictators but in two missing digits in computer date codes. Think about that—just two digits! The dreaded digital glitch that threatened to hurl our technologically dependent society into chaos was an early testament to the highly interwoven fabric of a globalized world.[16]

How Would the Cognitive Operating System Function in Practice?

A notional scenario can illustrate how a GenAI-powered cognitive operating system might function. Under this scenario, national security practitioners are dealing with an emerging geopolitical situation and prompt the large language model to provide insights into unforeseen second- and third-order effects of potential policy decisions and actions:

Background: In the autonomous region of Zephyria, a new political movement, the Aeolian Bloc, advocates for increased autonomy and challenges the central governmental authority. Intelligence reporting indicates possible foreign influence, yet specifics remain elusive. Social media in Zephyria is buzzing with dissent, and regional powers are taking an unusual interest in the developing situation.

Introducing the Cognitive Operating System: The security community uses its GenAI-powered cognitive operating system to synthesize strategic insights from vast data sources, including satellite imagery, communications intercepts, and open source intelligence. Personnel, steeped in strategic foresight and futures literacy, conduct horizon scanning, build emerging trend analysis, examine historical and cultural contexts, and pinpoint sources of disruption.

The Situation Unfolds: A sudden, unexplained electricity blackout in Zephyria's capital coincides with unusual stock trading in commodities endemic to Zephyria. In response, social media is rife with contradictory reports of a coup, an extraterrestrial event, and a targeted cyber attack.

GenAI's Role: The GenAI system identifies connections across these anomalies. It highlights the digital signature of a sophisticated misinformation campaign, correlates the trading anomalies with past economic warfare tactics, and pinpoints the cyber vulnerability exploited during the blackout.

Open-Ended Scenario for Planners: National security teams examine the GenAI's findings, but the intent behind these disruptions remains unclear, as does the identity of the instigators. The teams must now anticipate possible ***outcomes***—from peaceful demonstrations to a full-blown geopolitical crisis—considering both internal and external actors' motivations.

Key Questions for the Intelligence and Military Communities To Assess:

1. How might different foreign actors benefit from instability in Zephyria?
2. What are the blackout's second- and third-order effects on regional security and global markets?
3. Which indicators would suggest a misinformation campaign as a prelude to a larger strategic move?
4. How can we differentiate between genuine social unrest and synthetic agitation fueled by external forces?
5. In what ways might our response to this event set a precedent for future crises?

Leaving the scenario open-ended and focusing on these probing questions will enable planners to stimulate anticipatory thinking and strategic foresight and encourage a deeper engagement with the complex dynamics of modern geopolitics.

Implications: Rewiring the Hardware—Not Just a New Smartphone Application

It is still largely business as usual in the national security enterprise, even after the strategic failures in Iraq and Afghanistan, a global pandemic, and resurging conflicts in Ukraine and the Middle East. Without a cognitive operating system able to contextualize and anticipate the complexities of our digital age, we are sailing blind in a storm of our *own* making. National security personnel must be able to connect disparate pieces of information, identify patterns and anomalies, and craft potential future scenarios in tandem with GenAI tools.[18]

Although it is tempting to try to develop a "smartphone app" solution that promises quick fixes to deeply rooted problems, we must upgrade our "hardware" of human capital, providing our people with a cognitive transformation that transcends the superficial. Doing so would involve the cultivation of a workforce both technologically proficient with GenAI tools and intellectually robust—one capable of navigating the intricacies of an increasingly complex world with strategic foresight and nuanced understanding. This new operating system of the mind, integrated seamlessly into the daily operational culture of our institutions, would greatly enhance strategic thinking and problem-solving capabilities.

We must overhaul training and education in this GenAI-dominated era, shifting from quantity-driven analysis to quality-driven interpretation. Training programs must focus on developing deep regional and subject matter expertise, critical thinking skills, and an understanding of strategic foresight methodologies to create a work force more adept at interpreting and contextualizing information in a rapidly changing global landscape.

This century's volatile opening chapters presage more upheaval ahead as converging disruptions plunge the world deeper into polycrisis. We can continue to default to outdated strategic paradigms that fuel endless wars, or we can fundamentally transform the national security enterprise's "cognitive operating system." The imperative for change is clear. We must equip our military and intelligence communities with tools more attuned to the complex threat landscape they navigate. By embracing agile, informed, and anticipatory thinking, we can cultivate the foresight needed to preempt crises, not just react to conflicts. The digital age demands leaders who can position the workforce not only to win today's wars but also prevent tomorrow's. This requires investing in our people as much as the technology they wield. Their minds—not just materiel—will determine success in future conflicts.

Dr. Jake Sotiriadis is director of NIU's Center for Futures Intelligence in the Caracristi Institute and director of Operations and Engagement for NIU's iRES (Intelligence, Research, Education, and Solutions) laboratory.

If you have comments, questions, or suggestions for a *Research Short* topic or article, please contact the NIU Office of Research at **NIPress@niu.odni.gov**.

Endnotes

1 "This Is Why 'Polycrisis' Is a Useful Way of Looking at the World Right Now," World Economic Forum, March 7, 2023, https://www.weforum.org/agenda/2023/03/polycrisis-adam-tooze-historian-explains/.

2 Franciso Guzman, "Explosion Near Pentagon Never Happened, Officials Say, After Fake AI Picture Circulated Online," *USA Today*, May 24, 2023, https://www.usatoday.com/story/news/nation/2023/05/23/fake-pentagon-explosion-picture-ai-generated/70247245007/.

3 Teresa Rivas, "An AI-Generated Pentagon Image Caused a Brief Panic in the Stock Market," *Barron's,* May 23, 2023, https://www.barrons.com/articles/ai-fake-pentagon-explosion-stock-market-fdaafd77.

4 Thomas Homer-Dixon et al., "A Complex Systems Approach to the Study of Ideology: Cognitive-Affective Structures, and the Dynamics of Belief Systems," *Journal of Social and Political Psychology*, 2013, vol. 1(1), 337–363.

5 "Understanding Operating Systems," University of Wollongong (Australia), https://www.uow.edu.au/student/learning-co-op/technology-and-software/operation-systems.

6 For more on strategic foresight methodologies, see: Wendell Bell, *Foundations of Futures Studies: Human Science for a New Era*, vol. 1, Transaction Publishers, 1997; James Dator, *World Futures Review*, vol. 7, no. 4, December 2015; Jennifer Gidley, *The Future: A Very Short Introduction* (Oxford, UK: Oxford University Press, 2017).

7 Jairus Grove, Jacob Sotiriadis et al., "Global Futures Report: Alternative Futures of Geopolitical Competition in a Post-Covid World," Headquarters, United States Air Force A5/7, June 2020, https://apps.dtic.mil/sti/pdfs/AD1108029.pdf.

8 M. Gupta et al., "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," *IEEE Access*, 2023, vol. 11, 80218–45.

9 Joe McKendrick and Andy Thurai, "AI Isn't Ready to Make Unsupervised Decisions," *Harvard Business Review*, September 15th, 2022, https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions.

10 D. Finkenstadt, T. Eapen, J. Sotiriadis, P. Guinto, "Use GenAI To Improve Scenario Planning," *Harvard Business Review*, November 30, 2023, https://hbr.org/2023/11/use-genai-to-improve-scenario-planning.

11 D. Finkenstadt, J. Sotiriadis, P. Guinto, T. Eapen, "Contingency Scenario Planning Using Generative AI," *California Management Review*, January 22, 2024, https://cmr.berkeley.edu/2024/01/contingency-scenario-planning-using-generative-ai/.

12 Department of Defense, "Summary of the Joint All-Domain Command and Control Strategy," March 2022, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

13 Jon Harper, "US Military Publishes New Joint Warfighting Doctrine," *Defensescoop*, September 13, 2023, https://defensescoop.com/2023/09/13/us-military-publishes-new-joint-warfighting-doctrine/.

14 Joint Chiefs of Staff, "Developing Today's Joint Officers for Tomorrow's Ways of War," May 1, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/education/jcs_pme_tm_vision.pdf?ver=2020-05-15-102429-817.

15 Joint Chiefs of Staff, "Developing Today's Joint Officers."

16 Frederick E. Allen, "Apocalypse Then: When Y2K Didn't Lead To the End of Civilization," *Forbes*, December 29, 2019, https://www.forbes.com/sites/frederickallen/2020/12/29/apocalypse-then-when-y2k-didnt-lead-to-the-end-of-civilization/.

17 R. Sun, ed., Cognition and Multi-Agent Interaction: From Cognitive Modeling to Social Simulation, (Cambridge, MA: MIT Press, 2006).

18 Finkenstadt, Eapen, Sotiriadis, Guinto, "Use GenAI To Improve Scenario Planning."