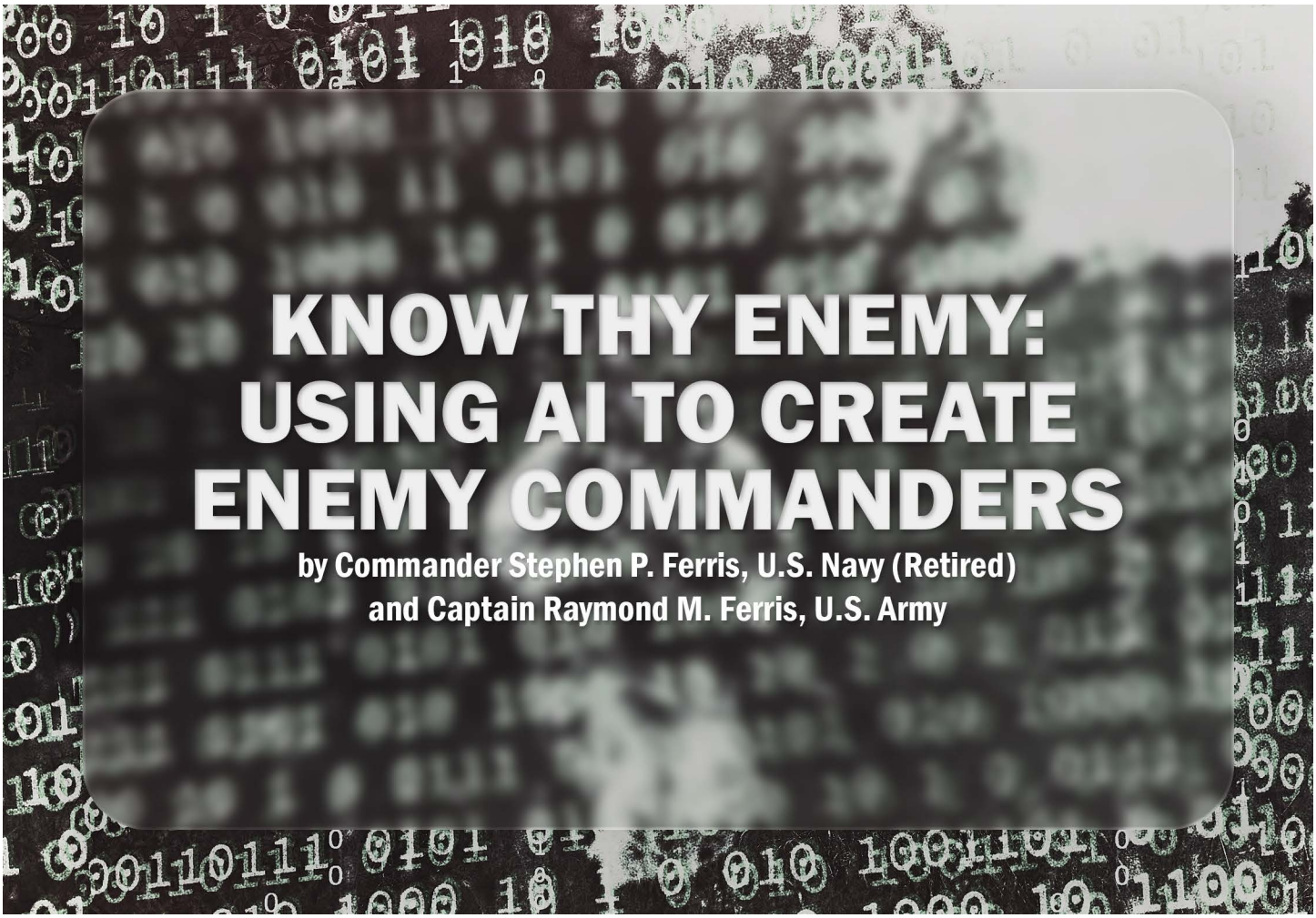

KNOW THY ENEMY: USING AI TO CREATE ENEMY COMMANDERS

by Commander Stephen P. Ferris, U.S. Navy (Retired)
and Captain Raymond M. Ferris, U.S. Army

Introducing the Digital Enemy Commander

Military intelligence faces unprecedented challenges in understanding adversary behavior in this current era of multi-domain warfare. One promising way forward is the use of artificial intelligence (AI), which is rapidly becoming the most transformative technology in military operations since the advent of digital communications, offering unprecedented capabilities to understand enemy intent and predict their behaviors. AI fundamentally reshapes how intelligence officers analyze threats, predict enemy actions, and support their commanders' decision-making. This essay explores a new application of AI for the intelligence officer: the development of an AI persona who can serve as the digital enemy commander or red team. This digital commander can reflect the tactics, strategies, and mindset of the opposing force, allowing intelligence professionals an unprecedented insight into adversary intentions and decisions.

Traditional intelligence analysis faces significant limitations that constrain its effectiveness. Human analysts, despite their expertise and intuition, struggle with inherent cognitive biases which can skew threat assessments and operational recommendations.[1] The information processing capacity of humans becomes increasingly insufficient when confronted with an abundance of data from satellite imagery, signals intelligence, human sources, and open-source materials.[2] Most critically, traditional intelligence methods fail to identify the decision-making patterns of adversaries who operate from fundamentally different cultural, ideological, or strategic frameworks.[3]

The creation of an AI agent who mimics the thinking of an adversary is a significant technological advancement, offering intelligence officers a valuable tool to anticipate enemy behaviors. These sophisticated AI agents can function as digital enemy force commanders, trained on comprehensive datasets of adversary behavior, doctrine, communications, and decision-making patterns. Unlike traditional analysis that simply examines previous enemy actions, these AI agents enable intelligence officers to anticipate the enemy, providing real-time insights into how adversary commanders might respond to dynamic battlefield conditions, strategic pressures, or friendly force actions.

This concept already exists in the private sector with companies employing AI executives or managers to model competitor decision-making processes or regulatory decision making.[4] Companies leverage sophisticated AI systems to analyze executive communication patterns, strategic announcements, and market responses to predict competitor responses. These business applications show the ability of

AI to discover complex human decision-making patterns and predict future actions based on historical data.

The integration of an AI-developed digital commander with current intelligence doctrine and best practices represents an evolutionary leap forward in the practice of military intelligence. These AI systems complement existing doctrinal frameworks by providing dynamic, data-driven insights that augment human analytical judgment. For the intelligence officer, these adversarial agents offer the ability to conduct virtual consultations with the enemy commander and receive an immediate enemy response to a proposed course of action, complete with military reasoning.

Using AI agents to simulate the decision-making of an enemy commander offers substantial benefits. The AI agent's ability to model specific adversarial thought processes, command preferences, and tactical doctrines results in enhanced predictive accuracy. These digital commanders reflect likely enemy responses to friendly force movements by using the cognitive frameworks and strategic priorities of actual opposing leaders. Another benefit is reduced analytical bias: the AI agent has the capacity to think from the adversary's perspective without the constraints of friendly force cultural or doctrinal assumptions. Real-time adaptive modeling allows these digital enemy commanders to evolve their decision-making as new intelligence is collected. This ability to adapt provides intelligence officers with dynamic threat assessments that reflect how adversary commanders might respond to developing situations. Strategic planning also improves through the AI agent's ability to role-play enemy decision-making across multiple military scenarios, resource allocations, and political developments.

"The human element remains critical in final decision-making while AI enhances both the quality and speed of information processing."

Digital Adversaries and Intelligence Doctrine

Current intelligence doctrine emphasizes the analysis of adversary capabilities, intentions, and operational methods through intelligence preparation of the operational environment (IPOE).[5] This analysis of the adversary centers on understanding enemy force structures, operational patterns, decision-making hierarchies, and adaptive capabilities. IPOE focuses on historical precedent analysis, war gaming simulations, cultural and behavioral profiling of enemy leadership, war gaming simulations, and red team exercises.

The U.S. military's red team tradition began with the Army War College's use of opposing forces in the early 1900s, evolved through World War II's strategic war gaming, and was refined during Cold War exercises like REFORGER and ABLE ARCHER.[6] These exercises employed human analysts and military personnel to think and act like enemy commanders. They attempted to replicate adversary decision-making processes, tactical preferences, and strategic posturing. The National Training Center at Fort Irwin institutionalized this approach through the Opposition Forces (OPFOR) program, where American units trained against forces employing Soviet tactics and equipment.

Red force exercises consistently show that human role-players, despite their expertise, face limitations in maintaining adversary perspectives over extended periods. Cultural biases, fatigue, and unconscious adoption of friendly force thinking compromise red team effectiveness.[7] Human cognitive limitations become apparent when processing large datasets from multiple intelligence sources. Time constraints during crisis situations often force analysts to rely on incomplete assessments.

AI adversary agents represent the natural evolution of the use of red force thinking in intelligence assessment. They consistently simulate the enemy's perspective through continuous learning, bias-free analysis, and unlimited processing capacity. AI adversary agents do not suffer the limitations of human red force commanders.

Intelligence doctrine recognizes that military intelligence personnel must continuously adapt their analytical approaches to anticipate adversary actions. Doctrine acknowledges that potential enemies represent sophisticated, thinking opponents with significant capabilities and resources. The existence of these adversaries who creatively respond to our actions necessitates a digital agent to model enemy behaviors in real time.[8]

AI opportunities within existing doctrine focus on areas where human-AI collaboration can enhance analytical capabilities rather than replace human insight. Digital enemy commanders can complement current practices by providing continuous behavioral modeling that updates in real time and processes multi-source intelligence beyond human capacity. They can also identify subtle correlations across vast datasets and generate multiple scenario predictions for strategic planning purposes. Doctrine compatibility ensures that AI agents support rather than supplant human intelligence analysts. The human element remains critical in final decision-making while AI enhances both the quality and speed of information processing.

Technical Foundation and Implementation

Digital enemy commanders represent a specialized application of AI designed to replicate specific enemy decision-making processes and strategic thinking patterns through sophisticated behavioral modeling techniques. These techniques integrate multiple AI technologies such as machine learning algorithms for behavioral pattern recognition, natural language processing for communication analysis, game theory models for strategic decision simulation, and reinforcement learning mechanisms for adaptive behavior modification.

The foundation for AI adversary modeling draws heavily from successful business intelligence applications where AI systems analyze senior executives' behaviors and competitive strategies. The Strategic Consortium of Intelligence Professionals (SCIP), the world's largest global intelligence association with over 15,000 members in 120 countries, emphasizes the growing importance of data-driven competitive intelligence in understanding executive decision-making patterns.[9] Business intelligence practices use AI to model competitor behavior by analyzing communication patterns, press releases, strategic announcements, financial decisions, and operational changes.

Business applications reveal several key insights applicable to military adversary modeling.[10] AI systems excel at identifying subtle patterns in executive communication that human analysts might miss, such as linguistic markers indicating strategic shifts or decision-making stress. Machine learning algorithms can correlate seemingly unrelated data points such as economic indicators, personnel changes, market pressures, and public statements to predict changes in corporate marketing or operational directions. Natural language processing analyzes leadership rhetoric for signals of policy shifts, risk appetite, and strategic priorities.

Training an AI agent to act like an enemy commander requires the collection and analysis of diverse data sources that reveal adversary decision-making patterns. Historical military operations provide foundational training data, including documented enemy tactical decisions, strategic choices, and operational adaptations across various conflict scenarios. Leadership communications, including speeches, military directives, doctrine publications, and strategic guidance documents, indicate cognitive frameworks and operational philosophies. Cultural and ideological materials, such as military education curricula, historical texts, and philosophical or political works that influence enemy thinking, provide essential context for understanding an adversary's worldview.

Intelligence databases containing years of enemy practices, response timelines, and adaptation strategies offer quantitative foundations for behavioral modeling. Economic and political decision-making records show how external pressures influence military choices. Communication patterns reveal leadership interaction styles, decision-making hierarchies, and information flow preferences. Exercise and training records from enemy forces imply preferred tactics, operational concepts, and adaptation capabilities.

Real-time data processing mechanisms employ distributed computing architectures that can scale with intelligence volume and complexity. Historical database integration provides contextual depth by incorporating decades of adversary behavior patterns, enabling digital agents to identify long-term trends and cyclical patterns in enemy decision-making easily overlooked by human observers. Social media and open-source intelligence adds contemporary behavioral indicators that complement traditional intelligence sources.

The computational foundation of digital adversary systems relies on sophisticated decision-making algorithms that enable complex behavioral modeling.[11] Bayesian networks manage uncertainty and probability distributions across multiple scenario possibilities. Neural networks provide complex pattern recognition capabilities for identifying subtle behavioral correlations. Decision trees model tactical choice hierarchies based on adversary doctrine and historical preferences. Monte Carlo simulations generate outcome probability assessments for strategic planning support.

Decision-Making Algorithms Defined

Bayesian Network: A type of graphical model representing probabilistic relationships among a set of variables. A Bayesian network is a visual map of cause-and-effect relationships that assist in making informed predictions.

Neural Network: Unlike Bayesian networks which rely on predefined relationships, neural networks, which are modeled on the human brain, learn relationships directly from raw data. These networks employ interconnected nodes organized into three layers: the input layer receives data; the hidden layer (i.e, the "brains" of the network) processes that data; and the output layer generates a prediction or conclusion.

Decision Tree: One of the most intuitive tools in machine learning, a decision tree is essentially a flowchart using a series of if-then-else rules to predict an outcome. At its simplest, a decision tree breaks complex problems down into smaller, more easily manageable decisions and produces a visual representation of the possible outcomes of each choice.

Monte Carlo simulation: These simulations use probability distributions to solve complex problems by using randomness and repetition to explore many possible outcomes—effectively predicting the future by running "what if" scenarios thousands (or millions) of times to estimate the likelihood of different results.

Behavioral modeling for creating a digital adversary focuses on three primary dimensions: cognitive architecture replication, cultural framework integration, and strategic preference modeling.[12] Cognitive architecture replication involves mapping individual adversary leaders' decision-making patterns, risk tolerance levels, and cognitive biases. For example, an

AI agent might incorporate a specific commander's documented preference for aggressive flanking maneuvers and willingness to accept high casualty rates, thus predicting bold tactical choices over defensive consolidation. Cultural framework integration incorporates social, economic, and political environmental factors that influence adversary behavior. A system modeling a clan-based society leader, for example, would include face-saving requirements, religious calendar constraints, and tribal balance considerations when predicting military decisions. Strategic preference modeling analyzes historical decision patterns to predict future choices under similar circumstances. As an example, an enemy commander who historically reinforces failing positions rather than withdrawing would likely repeat this pattern, allowing the digital adversary to predict the commitment of reserves rather than tactical repositioning.

Applications Across the Threat Spectrum

Digital adversaries demonstrate their versatility across the entire threat spectrum, from immediate tactical challenges to long-term strategic competition. These AI-powered agents adapt their modeling approaches to match the scope and complexity of different operational environments. This section describes how adversary simulation capabilities scale from battlefield-level decision support to national-level strategic planning.

- *Tactical intelligence support* provides immediate operational value through battlefield prediction and counter-strategy development. Unit deployment and movement pattern analysis provided by the digital enemy commander can identify enemy tactical preferences and likely courses of action. Identification of communications and logistics vulnerability reveals weak points in adversary operational systems. Real-time tactical recommendations provide commanders with response options based on evolving battlefield conditions.
- *Crisis response and conflict escalation* scenarios benefit significantly from the modeling of enemy intent. De-escalation strategy development involves predicting adversary responses to various diplomatic and military initiatives. For instance, it might model how a regional power responds to graduated economic sanctions versus immediate military action. Red line identification and boundary testing scenarios help commanders understand adversary tolerance levels and likely escalation triggers. Negotiation strategy optimization provides insights into adversary priorities and acceptable compromise positions. Unintended consequence prediction and mitigation identify potential second- and third-order effects of proposed actions, such as anticipating how arms sales to regional allies might trigger adversary military modernization programs or shift alliance structures.
- *Training and exercise applications* of digital adversaries enhance military preparedness through more realistic adversary simulation. Enhanced red team capabilities provide more sophisticated opposition forces for deployment in military exercises. Realistic adversary behavior simulation creates training scenarios that better prepare personnel for actual combat conditions. Digital enemy commanders can stress the decision-making of friendly forces and create highly challenging scenarios.
- *Counterintelligence operations* gain significant capability with the deployment of a digital enemy commander. This digital enemy acts as a virtual opponent, continuously challenging friendly counterintelligence assessments by simulating hostile intelligence intent and incorporating multi-domain threats. The digital adversary models enemy intelligence collection practices, such as predicting embassy personnel positioning or anticipating coordinated social media strategies. Through adversarial simulation, this digital enemy reveals potential deception campaigns by offering alternative narratives and cross-platform coordination that mirrors actual foreign intelligence behaviors. The virtual opponent validates double agent operations and source reliability by adopting the adversary's perspective to identify operational vulnerabilities and asset compromise indicators. Most critically, the digital enemy commander actively models adversary influence on operational timelines and predicts enemy responses to friendly countermeasures.
- *Strategic intelligence* can incorporate sophisticated digital agents to serve as force multipliers in adversary analysis and long-term planning. By analyzing resource allocation patterns, technology acquisition strategies, and force modernization priorities, digital agents can anticipate how adversaries will evolve militarily over time. This analysis extends beyond hardware to encompass policy and doctrine evolution, forecasting how an adversary's strategic posture might respond to geo-political and military developments.
- *Examining alliance structures and partnership networks* is key to understanding adversary behavior. The digital enemy can describe how adversary coalitions respond to strategic pressures and opportunities, revealing the web of relationships that shape collective decision-making. These agents can explain alliance politics, economic interdependencies, and shared strategic interests that influence how adversary blocs coordinate their responses to external challenges.

The sophistication of these digital agents becomes evident when assessing how economic and political decisions cascade into military action. Digital adversaries can predict the effects of economic sanctions, political transitions, or diplomatic

pressure on enemy military actions or likely countermoves. This capability also allows intelligence officers to anticipate second- and third-order effects before a decision is actually executed, enabling more informed strategic planning.

Mitigation Strategies for Implementation Challenges

Technical limitations present various challenges to adopting adversary digital agents in intelligence operations.[13] Data quality significantly limits AI system accuracy, particularly when historical data is incomplete, fragmented, or unreliable. Computational resource requirements for sophisticated behavioral modeling and prediction can quickly exceed available processing capacity. This is especially true when modeling complex, adaptive adversary networks. Further, model bias and accuracy concerns become critical when training datasets inadequately capture the full spectrum of variability in adversary behavior, tactics, and decision-making processes.

Adversary adaptation and countermeasures pose continual problems to the usefulness of digital adversary effectiveness. Enemies engaged in evasive attacks could attempt to deceive AI systems by developing new types of digital camouflage.[14] Sophisticated adversaries might deliberately alter their behavior patterns to confuse AI agents. Deception campaigns specifically designed to exploit AI vulnerabilities could compromise the accuracy of digital agents. Counter-AI technologies can enable adversaries to identify and neutralize friendly AI capabilities.

Operational challenges can create barriers that complicate the use of digital adversary agents across intelligence organizations. Over-reliance on AI recommendations risks degrading human analytical skills and intuition, potentially creating dangerous dependencies that erode the critical thinking capabilities of human analysts. This concern is compounded by the problem of integration with legacy intelligence systems, which requires new technical resources, specialized expertise, and extensive system modifications. Experienced analysts' resistance to training and adoption can slow implementation even further, as seasoned professionals often cite their own field experience in questioning the usefulness of AI-generated insights. Meanwhile, digital adversaries' real-time processing demands place enormous stress on the existing computing infrastructure, creating bottlenecks that can compromise operational effectiveness during critical intelligence gathering periods.

Human oversight also becomes increasingly difficult when AI agents rely on thousands of data points to draw conclusions, making it nearly impossible for human analysts to verify AI output accuracy.[15] The growing complexity of modern AI systems frequently exceeds human comprehension capabilities, creating significant accountability gaps in intelligence assessment processes. Successful integration, therefore, requires careful consideration of the existing analyst workflow while maintaining human judgment as the ultimate decision-making authority. This ensures that AI enhances rather than replaces human expertise in critical intelligence operations.

Effective mitigation strategies can successfully integrate digital adversary agents into intelligence operations as valuable tools for assessing enemy intentions and likely courses of action.[16] Technical challenges require targeted solutions that ensure system reliability and accuracy. Robust data validation protocols address incomplete historical intelligence by establishing quality thresholds and cross-referencing multiple sources. Classification safeguards prevent inadvertent disclosure by implementing automated security checks and human review processes. Scalable computing architectures accommodate sophisticated behavioral modeling without overwhelming existing infrastructure. Diverse training datasets capture the full spectrum of adversary behavior patterns across operational contexts and geographical regions.

Operational integration demands careful attention to analyst workload and organizational culture. Structured training programs help analysts understand system capabilities and limitations while building confidence in appropriate tool usage. Human-AI collaboration protocols can position digital adversary agents as tools for analytical support rather than decision-making replacements. Experienced analysts maintain primary authority over intelligence assessments while leveraging enhanced processing capabilities for complex pattern recognition. Gradual implementation phases further allow organizations to adapt to this new method of intelligence analysis.

Continuous improvement processes also ensure the long-term effectiveness of digital agents. Regular system updates address evolving adversary tactics and emerging threat patterns. Performance monitoring identifies degradation or potential countermeasures before they impact operations. Feedback mechanisms capture analyst insights to refine system accuracy and usability.

Conclusion

AI is fundamentally transforming how intelligence officers understand, analyze, and predict adversary behavior. This essay focuses on how AI can be used to create digital enemy commanders, providing unprecedented insight into enemy intentions and behaviors. Creation of digital adversary agents represents more than technological advancement; it constitutes a major shift in military intelligence methodology that allows intelligence officers to understand and predict the behavior of enemy commanders.

The development of digital adversary agents offers intelligence officers the capability to engage in virtual consultations with enemy commanders, testing proposed courses of action and receiving immediate adversary responses. This use of AI

enables intelligence professionals to surpass traditional analytical limitations through literal adoption of adversary leaders' mindsets. The intelligence officer gains access to enemy thinking patterns, decision-making processes, and strategic preferences that can be used in real-time.

The implications of digital adversaries extend beyond the immediate tactical advantages they provide to intelligence officers. Intelligence officers supported by a digital enemy commander gain the capability to continuously analyze enemy behavior, predict adversary responses to friendly actions, and identify strategic vulnerabilities often missed by traditional analysis. Digital adversaries allow friendly forces to respond much faster to enemy actions, anticipate enemy intentions more accurately, and develop more effective strategic planning across all levels of military operations.

"As adversaries like China advance their own military AI capabilities, the United States and its allies must leverage these technologies to preserve their intelligence advantages."

The datasets required to develop a digital agent are comprehensive enough to ensure a high degree of reliability for the recommendations that they generate. As they learn through continuous exposure to new intelligence inputs and validation against actual enemy behavior, these digital agents become increasingly sophisticated representations of adversary command thinking.

For the modern intelligence officer, digital adversary agents represent an indispensable tool for achieving analytical superiority in the global security environment. As adversaries like China advance their own military AI capabilities, the United States and its allies must leverage these technologies to preserve their intelligence advantages. The integration of digital agents with intelligence doctrine provides a foundation for revolutionary improvements in understanding and countering enemy threats.

The future of military intelligence lies in the integration of human expertise with AI capabilities.[17] The intelligence officer is the interface between the insights of the digital adversary and command decision-making. Digital enemy commanders will become essential tools in the intelligence officer's tool set. They will provide new capabilities to anticipate an adversary's thinking and to predict enemy actions at a level of accuracy impossible with traditional intelligence analysis. This transformation positions military intelligence at the forefront of the technological innovations that will shape the future of 21st century warfare.

Endnotes

1. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (27 September 1974), 1124-1131, https://www.science.org/doi/10.1126/science.185.4157.1124. Human decision-making is systematically influenced by numerous cognitive biases that can lead to errors in judgment and analysis. Kahneman and Tversky's foundational research identified key heuristics including confirmation bias (seeking or giving undue weight to information that confirms existing beliefs), availability heuristic (overweighting easily recalled information), and representativeness heuristic (judging probability by similarity to mental prototypes); Daniel Kahneman, *Thinking, fast and slow* (Farrar, Straus and Giroux, 02 April 2013). Additional biases include anchoring (over-relying on first information), overconfidence in one's abilities, loss aversion, and framing effects, which Kahneman later synthesized in his comprehensive analysis of dual-process thinking; Thomas Gilovich, Dale Griffin, and Daniel Kahneman, eds., Heuristics and Biases: The Psychology of Intuitive Judgment (Cambridge University Press, 08 July 2022). These systematic deviations from rational decision-making models demonstrate how intuitive judgment often leads to predictable errors.

2. Herbert A. Simon, "A behavioral model of rational choice," *The Quarterly Journal of Economics* 69, no. 1 (February 1955), 99-118, https://doi.org/10.2307/1884852. Human cognitive processing is constrained by limited attention, memory, and computational capacity, leading to systematic biases and heuristic-based decision-making rather than optimal choices.

3. David Robson, "How East and West think in profoundly different ways," *BBC*, 19 January 2017, https://www.bbc.com/future/article/20170118-how-east-and-west-think-in-profoundly-different-ways.

4. Pratik Kothari and Stephen P. Ferris, "Strategic Generosity: The Business of Political Contributions," *Social Science Research Network Electronic Journal* (28 April 2025), https://dx.doi.org/10.2139/ssrn.5241811. The authors use a sample of 4,949 digital corporate executives and find that executives primarily view political contributions as strategic investments that extract economic value and secure critical information to navigate policy landscapes.

5. Headquarters Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Government Publishing Office, 01 October 2023). IPOE is defined here as "the systematic process of analyzing the mission variables of enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations." The name change from "intelligence preparation of the battlefield" to "intelligence preparation of the operational environment" better reflects the multidomain nature of the operational environment.

6. David Alan Rosenberg, "Being 'Red:' The Challenge of Taking the Soviet Side in War Games at the Naval War College," *Naval War College Review* 41, no. 1 (Winter 1988): 81-93, https://digital-commons.usnwc.edu/nwc-review/vol41/iss1/7/; Micah Zenko, *Red Team: How to Succeed By Thinking Like the Enemy* (Basic Books, 2015).

7. Headquarters Department of the Army, *The Red Teaming Handbook*, 9th ed. (U.S. Army, 2024, distribution limited).

8. FM 2-0, *Intelligence*, 1-1—2-35.

9. “Strategic Consortium of Intelligence Professionals (SCIP),” SCIP, https://www.scip.org/. Originally called the Society of Competitive Intelligence Professionals, SCIP was founded in 1986 to promote competitive, market, and strategic intelligence practices in enterprise, academia, and government. This nonprofit organization provides education, certification programs, networking opportunities, and best practices for legal and ethical business intelligence collection and analysis, serving as the premier advocate for intelligence-driven decision-making.

10. Pratik Kothari and Stephen P. Ferris, “Personality-Driven Procurement: AI Executives and Strategies for Federal Contracting” (Working Paper, University of North Texas, 2025). While Kothari and Farris (2025) focus on strategies followed by CEOs to gain advantages in the federal contracting process, in this paper the authors survey a sample of digital CEOs to understand the reasons for corporate donations to political candidates.

11. Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. (Pearson, 08 May 2020).

12. Iuliia Kotseruba and John K. Tsotsos, “40 Years of Cognitive Architectures: Core Cognitive Abilities and Practical Applications,” *Artificial Intelligence Review* 53, no. 1 (2020), 17-94, https://psycnet.apa.org/doi/10.1007/s10462-018-9646-y; Aaron J. Barnes, YuanYuan Zhang, and Ana Valenzuela, “AI and Culture: Culturally Dependent Responses to AI Systems,” *Current Opinion in Psychology* 58 (August 2024), https://doi.org/10.1016/j.copsyc.2024.101838.

13. Adib Bin Rashid, Ashfakul Karim Kausik, Ahamed Al Hassan Sunny, and Mehedy Hassan Bappy, “Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges,” *International Journal of Intelligent Systems 2023*, no.1 (2023), http://dx.doi.org/10.1155/2023/8676366.

14. Digital camouflage involves masking authentic signals, communications patterns, and behavioral signatures to deceive adversary AI systems and digital personas. Techniques include spoofing metadata, generating synthetic noise, mimicking benign traffic patterns, and creating false digital footprints that obscure genuine operational activities from automated detection and analysis algorithms.

15. Yavar Bathaee, “The Artificial Intelligence Black Box and the Failure of Intent and Causation,” *Harvard Journal of Law & Technology* 31, no. 2 (Spring 2018), 889-938, https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf.

16. Anthony King, “Digital Targeting: Artificial Intelligence, Data, and Military Intelligence,” *Journal of Global Security Studies* 9, no. 2 (June 2024), https://doi.org/10.1093/jogss/ogae009.

17. Michael Mayer, “Trusting Machine Intelligence: Artificial Intelligence and Human-Autonomy Teaming in Military Operations,” *Defense & Security Analysis* 39, no. 4 (2023), 521-538, https://doi.org/10.1080/14751798.2023.2264070.

CDR Stephen Ferris (retired) is a professor of finance at the University of North Texas. He holds a bachelor of arts from Duquesne University, a master of business administration and a doctorate from the University of Pittsburgh, and a master’s degree in strategic studies from the U.S. Army War College. He also holds diplomas from the U.S. Army’s Command and General Staff College and the U.S. Navy’s College of Naval Command and Staff. His last active-duty assignment was with the J-4 on the Joint Staff.

CPT Raymond Ferris is the counterintelligence operations officer for 2nd Military Intelligence (MI) Battalion, 66th MI Brigade (Theater). He previously served as assistant S-2 for the 1st Armored Division, Division Artillery and as the company executive officer for Bravo Company, 532nd MI Battalion, 501st MI Brigade (Theater).