An artist's rendition of the commencement of Operation Glowing Symphony, a broad, synchronized cyber and psychological operations attack conducted against terrorist and administrative operations of the Islamic State by elements of the U.S. military with other agencies' participation from 2016 to 2017. (AI image by Gerardo Mena, Army University Press)

Exploring Artificial Intelligence-Enhanced Cyber and Information Operations Integration

Brig. Gen. Russell E. McGuire, JD, Virginia Army National Guard
Maj. Andre Slonopas, PhD, Virginia Army National Guard
Capt. Edward Olbrych, Virginia Army National Guard

The integration of artificial intelligence (AI) into military information operations (IO) cannot be left to the random evolution of a capability that is becoming already widely recognized by friend and foe alike as an essential component for support of all current and future multidomain operations.[1] Consequently, for U.S. forces and its allies, full-spectrum implementation of AI must be a very focused and carefully directed transition that is properly disciplined by exhaustive research to formulate and coordinate doctrine development, experimentation, applied lessons learned from actual practice, and then supported by robust resourcing in application.

Because there is no doubt that our adversaries are becoming more sophisticated in employment of AI in an information environment that is increasingly complex, leveraging AI's capabilities will not only be essential but will also be pivotal for maintaining the needed strategic edge and battlefield dominance to achieve success in the future. The potential capability of AI is such that failure by the United States to achieve AI dominance on the global stage will almost surely result in strategic failure for it and its allies in any future conflict.

After providing a brief historical summary of IO for context, this article will examine some specific applications and implications of AI in IO, offering insights into how it can be effectively employed to enhance the effectiveness of military campaigns. Given the limitations of an article-length work, it explores the impact of AI on modern IO by focusing on the lessons gleaned from two significant case studies: Operation Glowing Symphony, overseen by Joint Task Force (JTF) Ares, a real-world operation that was key to the dismantling of the Islamic State (IS) of Iraq and Syria in the late 2010s; and Cyber Fortress, an exercise series introduced in 2021 that grew directly out of lessons gleaned from major offensive and defensive cyber operations against IS and elsewhere in the Global War on Terrorism.

Past Precedent and Future Use of Information as Weapon

The use of information to influence, mislead, disrupt, or otherwise affect the enemy's decision-making and capabilities has been a cornerstone of military strategy throughout history.[2] Commanders have long understood that controlling the flow of information shapes the final outcomes of conflicts, making it an essential component of military operations.[3] From the ancient strategies of Sun Tzu, who emphasized deception and the use of spies, down to the complex psychological operations through the Cold War, Desert Storm, and the Global War on Terrorism, and currently in the Russia-Ukraine war, the competing struggle for information has remained a critical component of warfare.[4]

Notwithstanding, historically, the greatest challenge to what we broadly refer to as information operations has always been the formidable prospect of sorting through collected information in a timely fashion to distinguish important data from the less important and the unimportant. In that process, the major common impediment down through the history for exploitation of information effectively for various purposes has been the nagging challenge of speed in processing (i.e., creating an effective process for sorting rapidly through the information collected to distinguish the most salient data from the less relevant within the extreme limitations in the time frame for which analysis is needed).

Key features of anticipated modern warfare are rapidly evolving in such a manner as to often make some of the already inherent problems of information analysis harder rather easier.[5] For example, the ability to collect great amounts of data is easier than ever before, but the fact that the process has resulted in much greater amounts of information being collected than ever before makes the problem of sifting through and making sense of such massive quantities of accumulated data qualitatively more difficult given the tight deadlines for decision-making imposed by the increasing speed and pace of unfolding operations in the modern era. The problem has only been exacerbated by the rapid advances of computer technology in the first quarter of the twenty-first century that have dramatically increased even further the capability to collect vastly greater amounts of information than previously. The result is that it is now essentially impossible to effectively process and analyze the massive quantities of information now collected using just the traditional means of "hands on" human analysis even with the assistance of legacy computer systems.

Concurrently, irrespective of the challenges posed by technological advances related to information, reliance on traditional kinetic operations in conflicts

has been increasingly augmented and sometimes even supplanted by operations in the information domain, shifting the paradigm of war itself. This shift is largely driven by the exponential growth in digital communication technologies, the internet, and social media platforms that have radically transformed the landscape of information dissemination and manipulation.[6]

In this new emerging information era, the integration of advanced technologies using AI is indeed revolutionary—an often-abused word—that, in this case, is entirely accurate. AI-driven IO can automate and scale tasks that would be impossible for human operators to manage manually through traditional techniques and procedures.[7] Therefore, AI provides to the user for the first time in history the ability to effectively organize, categorize, and analyze previously unimagined vast amounts of data at unprecedented speeds—a genuine transformative revolutionary development not only in the domain of information but in the waging of warfare overall. Consequently, AI-enabled collection, collation, and analysis capabilities are increasingly recognized as a transformative force that must be incorporated for the timely planning and execution of military operations in an unprecedented manner, the boundaries of which are still unknown and provide a fertile field for expansion. The necessity for dramatically upgrading capabilities for processing information should highlight the need for investing in AI as a national strategic priority since it is already a crucial element for maintaining a strategic advantage in the modern global operational environment and in the future will only be more so.[8]

Additionally, the formulation of complex AI algorithms that enable rapidly winnowing through analysis of great amounts of data may in time mimic, replicate, or even supplant the arcane and mysterious factors thought to be behind the kind of human intuition military leaders have always cherished in the calculation of risk to improve decision-making that were previously believed to be outside the capabilities of machines and technology. In addition, such extreme sophistication in personality analysis may enable the weaponization of AI to create more effective psychological operations by providing real-time analysis and predictions regarding the predicted decisions of opponent forces based on comprehensive and exquisitely detailed data sets regarding the personality profiles and proclivities among the leaders of an adversary. Plausibly, in the exploitation of this advancement, AI has the potential to simultaneously generate and disseminate prodigious amounts of refined propaganda at the same time it manages complex targeted disinformation campaigns that exploit predicted human behavioral responses to influence

Brig. Gen. Russell E. McGuire is the assistant adjutant general of the Virginia Army National Guard. He holds a BA in English and history from the Virginia Military Institute, an MSS from the U.S. Army War College, and a JD from Western Michigan University. His previous assignments include commander of the 91st Cyber Brigade at Fort Belvoir, Virginia, and commander of the Information Operations Support Center in Fairfax, Virginia. He has deployed in support of Operations Iraqi Freedom and Enduring Freedom. His serves as the Louisa County commonwealth's attorney as his civilian occupation.

Maj. Andre Slonopas, Virginia Army National Guard, holds a PhD in aerospace engineering from the University of Virginia and is pursuing a second PhD in materials science and engineering at Johns Hopkins University. He is a former Presidential Management Fellow, and a graduate of the Command and General Staff Officer College, Cyber Operations Office Course, and the Information Operations Qualification Course, among other specialized information operations and cyber courses.

Capt. Edward Olbrych, Virginia Army National Guard, serves as a research electronics engineer at the U.S. Army Research Laboratory, focusing on electronic warfare technology. He is also an operations planner for the U.S. Army National Guard, where he has contributed to planning and execution of multiple joint international and interagency exercises. Olbrych's background includes contributions to defense projects at the U.S. Army Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance Center and at Lockheed Martin.

public opinion on social media. These applications highlight AI's potential to act as a force multiplier that amplifies the impact of traditional IO strategies. This just of itself would make it an indispensable tool supporting implementation of IO in a future conflict.[9]

Consequently, the capabilities AI provide are now essential in most forms of modern warfare where the speed and accuracy of information given to decision-makers will make the difference between success and failure. This means that the military's adoption of AI is not about incrementally improving existing legacy processes but about acknowledging and adjusting to a new paradigm shift in the nature of warfare overall that demands a revolutionary effort to employ new digital tools to vastly improve strategic and operational planning and analysis while also directly disrupting and degrading the information sharing and communication channels of the adversary on the world wide web.

The Rise of AI Applications in Military IO

As noted, AI technologies are transforming how militaries conduct information warfare, offering unprecedented capabilities and new challenges. AI can generate immense of amounts of information aligned to specific narratives, analyze massive volumes of data, and predict adversary maneuvers based on historical data and current patterns.[10] These capabilities enhance situational awareness and decision-making but also risk overwhelming decision-makers with information.

One of the most significant advantages of AI in IO is its ability to process and analyze large volumes of data quickly and accurately. AI can sift through satellite photos, real-time signal intercepts, and open-source intelligence data to identify patterns and trends that would be impossible for human analysts to detect. This capability dramatically improves situational awareness and decision-making, allowing military commanders to make better informed decisions in real-time.

However, as previously noted, the sheer volume of information needing analysis presents significant challenges. Without radical improvements to the tools needed for analysis, decision-makers risk being overwhelmed with data as they attempt to single out and act on the most critical information promptly. Such information overload can lead to decision paralysis, where commanders are unable to make timely decisions due to the overwhelming amount of data at their disposal that cannot be efficiently and usefully analyzed within the constraints of a highly sensitive timeline. AI in its many variants will be essential to remediate this challenge for decision-makers.

Additionally, weaponized AI can also generate deceptive information, leading adversarial AI to derive incorrect conclusions and mislead decision-makers. It can also facilitate analysis of the psychological characteristics of target groups, allowing for more effective and focused psychological operations.[11]

At the same time, defensive AI will be necessary when facing adversaries who may use AI-generated deepfakes and malevolent synthetic media to construct misinformation and morale campaigns aimed at adversely affecting friendly public opinion.[12] AI-generated videos and images can be used to both spread false information as well as undermine public trust in legitimate sources of information. Acknowledging this challenge, it is also necessary to recognize that the rapid advancement of AI technology means that deepfakes are becoming increasingly difficult to detect, making it challenging to counter these disinformation campaigns effectively.

Operation Glowing Symphony: A Pivotal Shift in Cyber and Information Warfare

Operation Glowing Symphony, part of the broader campaign against IS, represented a landmark in the use of the types of offensive cyber capabilities alluded to above to disrupt and degrade an adversary's information dissemination networks. This operation demonstrated how AI and cyber tools could be integrated to achieve strategic objectives in the information domain. It represented a pivotal shift in the integration of cyber and information warfare, marking a significant advancement in how these tactics are leveraged to combat adversaries like IS.[13] JTF Ares conducted operations as part of the broader campaign against IS, and this operation not only disrupted and degraded the group's ability to disseminate information, recruit members, and execute its digital communication strategies but also demonstrated the power of integrating offensive cyber capabilities with traditional IO to achieve strategic objectives.

Although many of the details about the Operation Glowing Symphony are not publicly releasable, the

operation began in 2016 and continued into 2017. The core of Operation Glowing Symphony was mounted from the U.S. Cyber Command's facilities, but the effects were dispersed against IS online infrastructure across the Middle East, Europe, and beyond. The success of the operations stemmed in large part to its seamless integration of cyber capabilities with traditional IO strategies. U.S. Cyber Command targeted servers, websites, and data centers used by IS, gaining control over their digital infrastructure. This allowed U.S. forces to disrupt IS's information capabilities while simultaneously implanting and executing friendly information aimed at the same audiences. By combining these approaches, the operation effectively neutralized IS's ability to influence and recruit through digital means. On the day of the operation multiple teams executed their scripts within a ten-minute window after getting the final go-ahead. They targeted various parts of IS's media network, including servers, social media accounts, and email addresses. The operation was described as a "symphony of destruction," systematically disabling and disrupting key parts of IS's digital presence.[14]

This integrated approach illustrates the evolution of modern warfare, where the boundaries between cyber operations and IO are increasingly blurred. Traditional IO focuses on influencing, disrupting, corrupting, or usurping the decision-making processes of adversaries while protecting friendly decision-making processes.[15] When these principles are combined with advanced cyber capabilities, the effectiveness of IO is significantly amplified. Cyber operations can directly manipulate the information environment, creating opportunities to insert counternarratives and disrupt adversary communications in real-time.

Additionally, one of the key innovations of Operation Glowing Symphony was its strategic use of friendly information to counter IS's propaganda. By infiltrating IS's digital platforms, U.S. cyber forces were able to not only halt the spread of IS's messages but also replace them with content that supported U.S. objectives. This proactive dissemination of friendly information helped to undermine IS's credibility and influence, sowing confusion and doubt among their supporters.

The U.S. ability to implant friendly information within enemy networks demonstrates a sophisticated understanding of the psychological aspects of warfare. Instead of merely silencing the adversary, the operation turned IS's own platforms against them, using them as channels to broadcast messages that contradicted and discredited the group's narratives. This tactic not only disrupted IS's recruitment efforts but also eroded their support base by providing alternative viewpoints and information that challenged their propaganda.

Operation Glowing Symphony also highlighted the effectiveness of using cyber capabilities to disrupt adversary IO.[16] By targeting the critical infrastructure that IS relied on for communication, U.S. Cyber Command was able to dismantle the group's digital networks. This disruption hindered IS's ability to coordinate attacks, recruit new members, and maintain their online presence.

The operation employed advanced hacking techniques to penetrate IS's defenses and manipulate the data and communications transmitted. This level of disruption required a deep understanding of both the technological and informational aspects of IS's operations. By effectively severing IS's communication lines, U.S. forces were able to isolate the group, making it difficult for them to sustain their operations and reach their audience.

Operation Glowing Symphony represented a watershed moment in the integration of cyber and information warfare. By successfully disrupting IS's digital communication networks and leveraging friendly information to counter their propaganda, U.S. Cyber Command has demonstrated the power and potential of combining cyber capabilities with traditional IO strategies.[17] This operation not only highlights the effectiveness of integrated approaches in modern warfare but also sets the stage for future innovations in the field. As the digital battlefield continues to expand, the principles and tactics employed in Operation Glowing Symphony will be crucial in guiding the evolution of cyber and information warfare.

Previous page: An artist's rendition of Operation Glowing Symphony attacks against terrorist operators during 2016 and 2017 that included hacking into Islamic State cell phones, computers, and other devices for the purpose of covertly stealing information, altering information, interrupting communications, and sowing confusion by misleading and promoting distrust among enemy belligerents with targeted propaganda. (AI image by Gerardo Mena, Army University Press)

Amplifying Cyber/IO with AI: A Cyber Fortress Case Study

Cyber Fortress is an exercise series that began in 2021 and is sponsored by the Virginia Department of Emergency Management in collaboration with the National Guard and other federal and private partners that was a direct outgrowth of the success of Operation Glowing Symphony. It is a powerful idea of a proactive cybersecurity relationship between private and public partners for the defense of the homeland. At present, Cyber Fortress is an annual event held in Virginia Beach that brings in dozens of participants from the federal and state government, and uniformed partners, and representatives from private, critical infrastructure, and academe.

The Cyber Fortress exercise involves a comprehensive simulation of digital and information environments, allowing military and civilian participants to practice and refine their IO strategies in a controlled setting. It showcases the evolving nature of information warfare training and preparedness.[18] The inclusion of AI in these exercises underscores its importance in future military operations and highlights the need for continuous adaptation and innovation.

Exercise Objectives Including Expanding Concepts for Employing AI

This exercise involves a comprehensive simulation of digital and information environments, allowing military and civilian participants to practice and refine their IO strategies in a controlled setting. The inclusion of AI in these exercises underscores its importance in future military operations and highlights the need for continuous adaptation and innovation.

The exercise examines and applies in various scenarios the lessons derived from the successes of Operation Glowing Symphony but also expands on the lessons learned to enhance consideration of additional steps for the defense of critical infrastructure. In doing so, it continues to explore and demonstrate the efficacy of AI in both cyber and IO. By leveraging emerging artificial intelligence, Cyber Fortress has not only improved domestic cyber defense capabilities but also has expanded consideration of complex scenarios involving extensive IO to create a more robust and adaptive response framework.

One of the main goals of the current Cyber Fortress is to use new AI tools in cyber security and IO. AI enables humans to assess network traffic, find anomalies and trends in large datasets, and react to events faster and more accurately than "unarmed" human analysts. AI-driven systems make it easier to find and stop cyber threats. These AI systems analyze data in near-real time incessantly, so any possible threats are found and stopped before they have an opportunity to do extensive damage. One important feature of AI is that it frees up human operators to make more important strategic decisions by automating routine tasks that would otherwise be time-consuming and debilitating in terms of slowing reaction time to events. This makes protecting critical infrastructure more efficient and efficacious.

In Cyber Fortress, AI is also used extensively to exercise both offensive and defensive IO. For hostile purposes, AI technologies allow customizable information campaigns as well as the creation of realistic fake media and changes to messages based on real-time feedback. Because of these features, red teams can run complex IO campaigns that can successfully distract, trick, and sway their targets.

Cyber Fortress also uses the exercise area to gather information about its users, which is then used to teach advanced machine learning algorithms. This method is based on data, which makes sure that AI systems keep learning and become better, which makes them more useful over time. The AI algorithms can find patterns and trends by looking at how people act and react to information. This makes it easier to predict and deal with future threats. In the ever-changing world of cyber and information warfare, this process of constant learning is essential for staying ahead of the enemy.

The main goal of Cyber Fortress is to create human skills that are enhanced by machines and can work well with limited funds. Cyber Fortress aims to improve the skills of human workers by integrating AI tools that will help them handle more complicated cyber and IO. This partnership between people and AI makes sure that tasks are done quicker with fewer errors, using the best parts of both human intelligence and machine accuracy.

Red Team versus Blue Team in AI-Driven IO Campaign Simulations

In Cyber Fortress, red teams employ AI to execute intricate and aggressive IO. Their goal is to disseminate

Cyber and information operators undergo training in preparation for Cyber Fortress, a cyber-information operations exercise for the defense of critical infrastructure, in July 2024 at State Military Reservation near Virginia Beach. (Photo courtesy of Virginia National Guard Public Affairs)

disruptive information to sow distrust and panic among the public. They use AI-driven algorithms to create messages in multiple languages, embedding cultural and ethnic nuances to ensure messages resonate deeply with various ethnic groups in the United States.

Red teams also use AI for adaptive messaging and real-time feedback, monitoring public reactions to adjust messaging accordingly. AI-generated chat conversation generators post comments across digital platforms, engaging in online discussions to influence public opinion and amplify disinformation campaigns.

The use of AI for adaptive messaging allows red teams to continually refine their tactics based on real-time feedback. By monitoring public reactions to their messages, they can identify which narratives are gaining traction and adjust their strategy accordingly. This adaptive approach ensures that the red teams' information campaigns remain effective and relevant, continually influencing public opinion and deepening divisions within the digital discourse.

Blue teams counteract these sophisticated operations with their AI-driven strategies. They rapidly generate accurate and reliable information to mitigate false narratives and employ AI for language translation tasks to monitor and counteract misinformation across diverse linguistic spectrums.

During Cyber Fortress, the Information Operations Support Cell (IOSC) serves as the analytical and strategic hub for blue teams. The IOSC oversees the information environment, utilizing advanced AI algorithms for natural language processing, sentiment analysis, and pattern recognition to identify and address deceptive content.

The IOSC's use of AI in natural language processing and sentiment analysis allows it to quickly identify the underlying strategies of the red team's campaigns. By analyzing target demographics, message frequency, and thematic content, it can tailor its countermeasures more effectively, ensuring rapid and strategically targeted responses. This capability is vital in maintaining

the integrity of information within the exercise and safeguarding the digital information landscape from corruption by falsified narratives.

Blue teams also use AI to develop proactive strategic communication plans, customizing content dissemination based on audience analysis. This approach ensures counternarratives reach the right people effectively.

language are getting smart enough to create and share believable narrative content on their own at a scale and speed that humans can't match.

In terms of strategy, the continued use of AI in military operations will have a huge impact on world politics. Information campaigns that use AI could lead to a new type of warfare in which digital battles happen and drive public opinion and national policies without any physical confrontation. Countries that are very good at AI could gain significant leverage in international relations through influence operations. This could start a new arms race based on who has the best and most efficient "intelligence."

> Information campaigns that use AI could lead to a new type of warfare in which digital battles happen and drive public opinion and national policies without any physical confrontation.

Ethical considerations like privacy, transparency, and accountability are paramount in AI utilization.

Understanding that different demographics consume information differently, blue teams use AI to customize the dissemination of their content. AI algorithms determine the most effective channels and formats for different audiences, ensuring that counternarratives reach the right people in the right way. This targeted approach enhances the effectiveness of the blue teams' information campaigns, helping to prevent the spread of harmful misinformation and build resilience within the public against future disinformation campaigns.

Emerging Technologies and Future Applications

There are monumental changes ahead for the future of AI in military IO. New technologies will make capabilities more accessible and will drive strategic changes in military operations. Advanced AI systems can handle unfathomable amounts of data and make complex psychological profiles, predictive models, and information campaigns that run themselves. These models can predict possible threats and make computerized responses to information campaigns. This gives military strategists a level of understanding and foresight that has never been seen before.

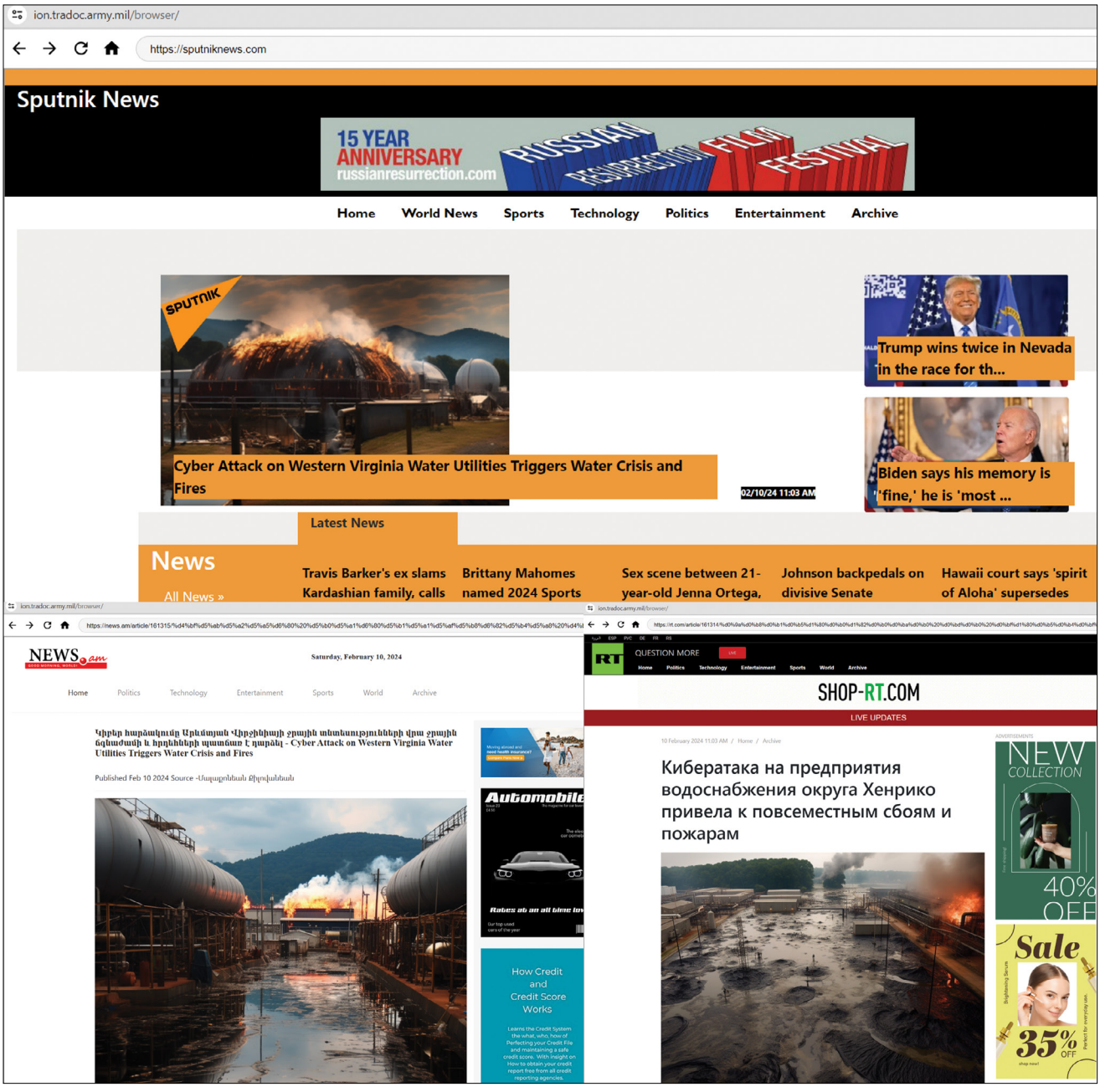
Using AI in deep learning and neural networks is one of the most important steps in technology development. This technology makes it possible to make a huge number of synthetic media that look and feel very real. This gives psychological operations a strategic edge. Also, tools that use AI to process and generate natural

Also, the automated tracking and analysis features of AI systems are very important for finding fake news and strange behavior quickly. These AI systems constantly look through digital interactions and media to find and flag possible threats or campaigns of false information. The unsupervised analysis of voluminous data, however, runs the risk of mislabeling legitimate information and amplifying false narratives. Hence, the human interaction assisted with AI is still required. This automated watchfulness improves defenses and makes sure that information activities are honest and work well. So, the future of AI in military IO isn't just about new technology, but it's also about making sure that strategic decision-makers always have the most up-to-date information and fighting new digital threats in a world that is becoming more and more linked.

Unsettled Ethical and Privacy Concerns in AI-Driven IO

As AI becomes more integrated into military IO, ethical considerations must be at the forefront of its deployment. The use of AI in creating and disseminating information raises significant ethical questions, particularly regarding privacy, transparency, and accountability.

The ability of AI to process and analyze vast amounts of data raises significant privacy concerns. AI systems



AI-generated images and narratives in multiple languages were developed as part of the information campaign during Cyber Fortress 24. (AI-generated images by authors via MidJourney; text generated by ChatGPT)

can collect and analyze data from various sources, including social media, communications, and other digital platforms, to identify patterns and trends. While this capability is invaluable for IO, it also raises concerns about the privacy of individuals whose data is collected and analyzed. Ensuring that AI systems are used responsibly and that data collection adheres to privacy laws and regulations is crucial. This involves implementing strict data governance policies and ensuring that data is anonymized and used only for legitimate purposes.

Furthermore, military use of AI must be scrutinized to prevent potential abuses. The aggregation of personal data can lead to unintended consequences, such as the targeting of individuals based on their digital footprint. Safeguarding personal information and preventing misuse requires robust security measures and continuous oversight.

Transparency in the use of AI for IO is essential to maintain public trust and ensure ethical conduct. The

creation and dissemination of information using AI must be transparent, with clear guidelines on how AI is used and what data is collected. Transparency also involves informing the public and relevant stakeholders about the objectives and methods of AI-driven operations. This can help demystify AI technologies and build public confidence in their use.

Accountability is another critical aspect of ethical AI deployment. There must be clear lines of responsibility for the actions taken by AI systems. Human oversight is necessary to ensure that AI-generated content is accurate and ethical and that any misuse of AI is promptly addressed. Establishing accountability frameworks can help monitor and evaluate the impact of AI systems, ensuring that they are used in ways that align with ethical standards and legal requirements.

The use of AI in warfare, particularly in IO, raises ethical questions about the manipulation of information and the potential for psychological harm. AI's ability to create realistic deepfakes and synthetic media can be used to manipulate public opinion and spread false information. The ethical implications of using AI in this manner must be carefully considered, and guidelines must be established to ensure that AI is used responsibly and ethically in military operations.

Ethical guidelines should address the potential for AI to be used in ways that could deceive or manipulate people, leading to unintended psychological or social consequences. For example, the use of deepfakes in propaganda can undermine trust in legitimate sources of information and contribute to social instability. Ethical frameworks must ensure that AI is not used to exploit vulnerabilities in human cognition and psychology in ways that are harmful or coercive.

Conclusion

AI in U.S. military IO is a strategic need for contemporary battlefield dominance. AI can analyze vast datasets and automate difficult psychological functions, transforming IO. Successful AI use requires a comprehensive and flexible strategy that combines innovation, strategic vision, and ethical responsibility. The U.S. military must invest in AI as a tool for efficiency and a transformational force influencing combat as the digital battlespace changes. This necessitates a move from existing paradigms to an AI-driven approach that prioritizes quick decision-making, agility, and cyber-information warfare integration. Responsible implementation also requires addressing data privacy, algorithmic bias, and AI abuse. The adoption of AI in IO will define military operations. It offers unprecedented opportunities to influence the global information ecosystem, prevent new dangers, and protect national security. In a constantly changing battlefield, the military's capacity to innovate, cooperate, and adapt will determine the effectiveness of this integration. ■

The authors would like to acknowledge ChatGPT's invaluable assistance, which provided critical insights and guidance throughout the writing process. AI's ability to process and generate informative content has been indispensable in shaping this article. The authors would also like to sincerely thank all the finite and ordinary human readers and colleagues who provided feedback and suggestions. Your perspectives and insights have been invaluable in ensuring the comprehensiveness and accuracy of this article.

Notes

1. Sam Kriegler, "Artificial Intelligence Guided Battle Management: Enabling Convergence in Multi-Domain Operations" (master's thesis, U.S. Army Command and General Staff College, 21 May 2020), https://apps.dtic.mil/sti/citations/trecms/AD1159377.

2. Fabian Villalobos and Scott Savitz, "Assemble the Bodyguard of Lies: Strengthening US Military Deception Capabilities," Modern War Institute, 11 April 2024, https://mwi.westpoint.edu/assemble-the-bodyguard-of-lies-strengthening-us-military-deception-capabilities/.

3. David S. Alberts and Richard E. Hayes, "Power to the Edge: Command ... Control ... In the Information Age" (Command and Control Research Program, Office of the Assistant Secretary of Defense, 1 January 2003), https://apps.dtic.mil/sti/citations/ADA457861.

4. Michael I. Handel, "Intelligence and Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 122–54, https://doi.org/10.1080/01402398208437104.

5. Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Potomac Institute for Policy Studies, December 2007), 16–17.

6. Zeynep Tufekci, "Engineering the Public: Big Data, Surveillance and Computational Politics," *First Monday* 19, no. 7 (July 2014), https://doi.org/10.5210/fm.v19i7.4901.

7. Paul R. Daugherty and H. James Wilson, *Human + Machine: Reimagining Work in the Age of AI* (Harvard Business Review Press, 2018), 124–54.

8. Michael Horowitz et al., *Strategic Competition in an Era of Artificial Intelligence* (Center for a New American Security, 25 July 2018), https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence.

9. Eberhard Hechler, Martin Oberhofer, and Thomas Schaeck, *Deploying AI in the Enterprise: IT Approaches for Design, DevOps, Governance, Change Management, Blockchain, and Quantum Computing* (Apress, 2020), https://doi.org/10.1007/978-1-4842-6206-1.

10. Benjamin M. Jensen, Christopher Whyte, and Scott Cuomo, "Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence," *International Studies Review* 22, no. 3 (2020): 526–50, https://doi.org/10.1093/isr/viz025.

11. James Johnson, ed., "Delegating Strategic Decisions to Intelligent Machines," chap. 8 in *Artificial Intelligence and the Future of Warfare* (Manchester University Press, 14 September 2021), https://doi.org/10.7765/9781526145062.00017.

12. Ignas Kalpokas, and Julija Kalpokiene, "Synthetic Media and Information Warfare: Assessing Potential Threats," in *The Russian Federation in Global Knowledge Warfare*, ed. Holger Mölder et al. (Springer Cham, 2021), 33–50, https://doi.org/10.1007/978-3-030-73955-3_3.

13. Christl A. Donnelly and Marcel Stolz, "JTF-ARES as a Model of a Persistent, Joint Cyber Task Force," *European Conference on Cyber Warfare and Security* 22, no. 1 (2023): 169–76, https://doi.org/10.34190/eccws.22.1.1200.

14. Jack Rhysider, host, *Darknet Diaries*, episode 50, "Operation Glowing Symphony," 29 October 2019, https://darknetdiaries.com/transcript/50/.

15. Donnelly and Stolz, "JTF-ARES."

16. Jeffrey D. Randall, "Crossing Borders in Cyberspace: Regulating Military Cyber Operations and the Fallacy of Territorial Sovereignty," *Army Lawyer*, no. 5 (2021): 82, https://tjaglcs.army.mil/Periodicals/The-Army-Lawyer/tal-2021-issue-5/Post/5798/No-3-Crossing-Borders-in-Cyberspace.

17. Tim Hwang, *Maneuver and Manipulation: On the Military Strategy of Online Information Warfare* (U.S. Army War College, 2019), https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1375&context=monographs.

18. Cotton Puryear, "Cyber Fortress Exercise Brings Together Federal, State, Private Sector Partners," Virginia National Guard, 10 October 2022, https://va.ng.mil/News/Article/3192161/cyber-fortress-exercise-brings-together-federal-state-private-sector-partners/.