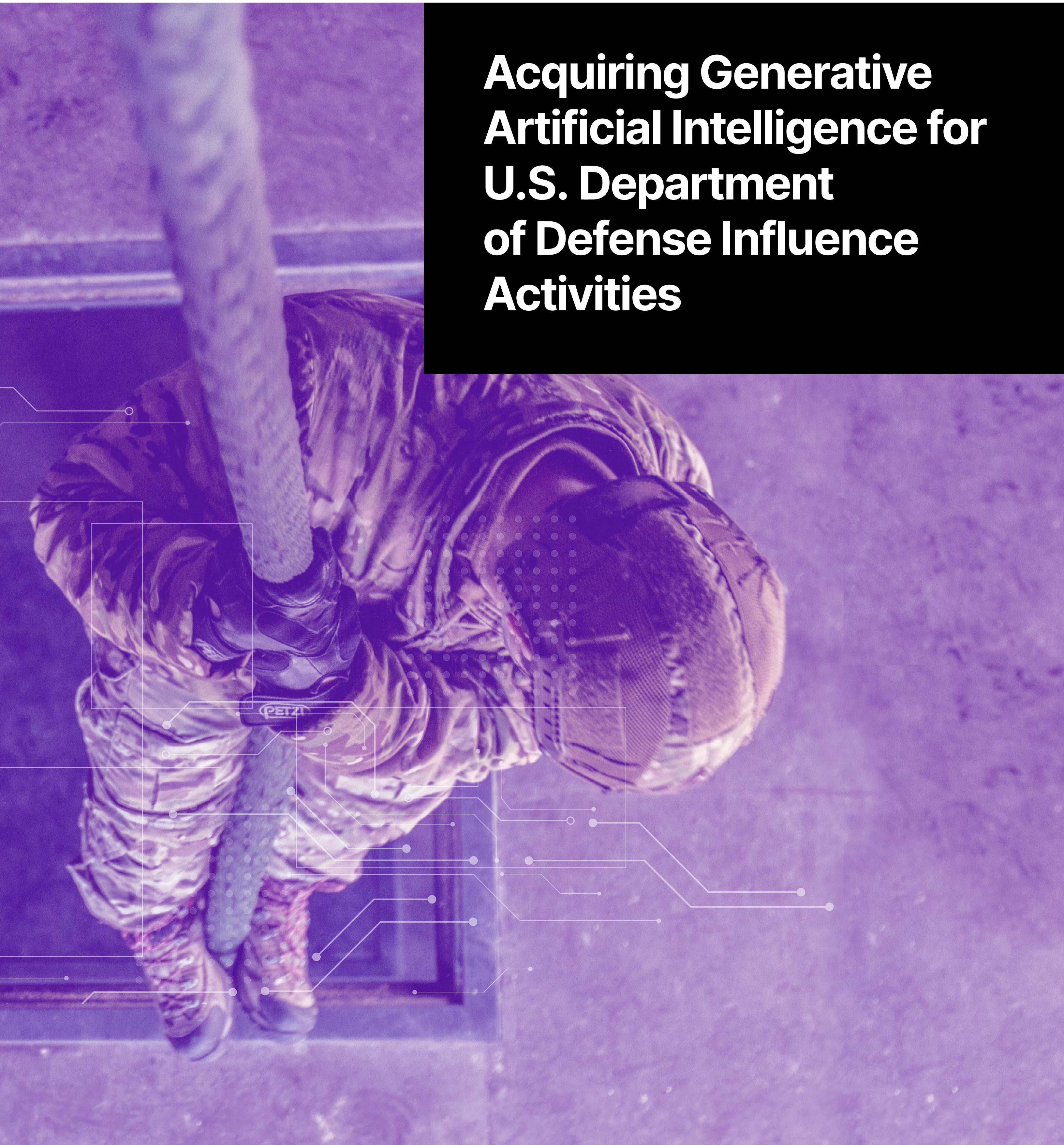
RESEARCH SUMMARY

Acquiring Generative Artificial Intelligence for U.S. Department of Defense Influence Activities



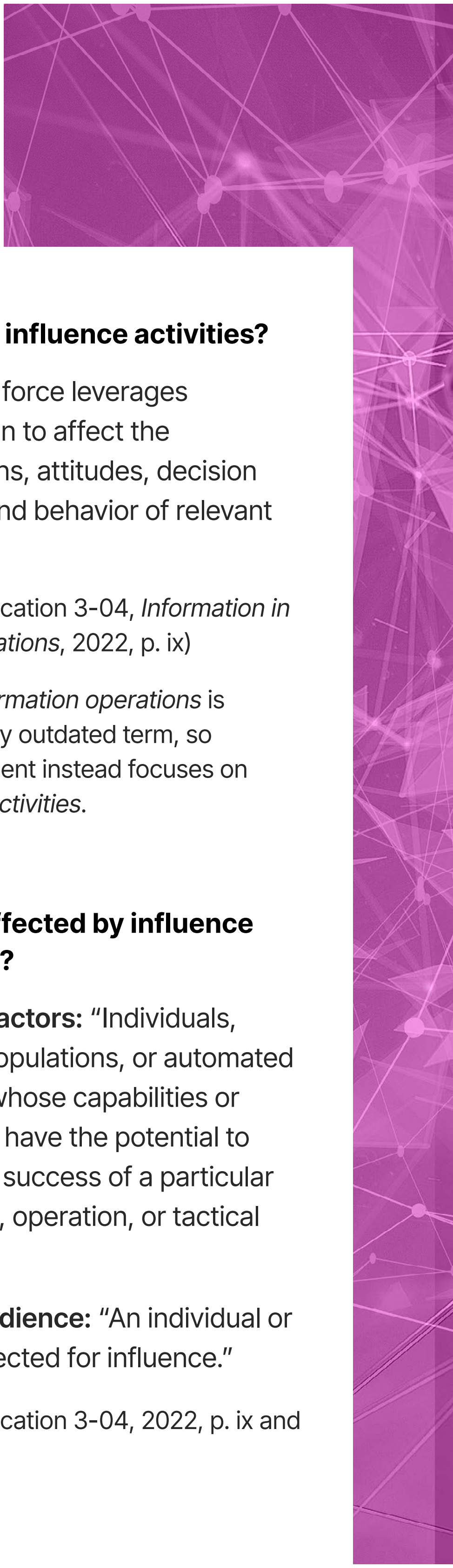
Key Findings and Recommendations

- To effectively compete and counter adversaries, the U.S. Department of Defense (DoD) needs to enable the influence community with generative artificial intelligence (AI), but there is a lack of substantial investment and unity of effort at present.
- Generative AI can dramatically improve analysis, operational planning, and assessment of influence activities; however, generative AI technology presents a tool, not the answer, for addressing DoD's rapidly evolving challenges.
- Effective acquisition of generative AI will require a strategic, flexible approach to ensure that users obtain the needed capabilities and a sustainment process that covers the spectrum of capabilities from enterprise to bespoke.
- No enterprisewide plan or strategy currently addresses generative AI implications or opportunities as they relate to influence activities or operations in the information environment.

Bottom line up front: Generative AI can improve analysis, operational planning, and assessment of influence activities, but it is *a tool*, not *the answer*, and maximizing its potential will take dedicated effort in several areas.

Background

The integration of generative artificial intelligence (AI) into influence activities, as with all uses of AI, presents enormous opportunities for scaling and automation of tasks. As strategic competition intensifies, particularly with China and Russia, generative AI presents a crucial tool for helping the U.S. military process vast amounts of data and produce high-quality content more efficiently. However, ad hoc efforts of the U.S. Department of Defense (DoD) to acquire, develop, and operationalize generative AI capabilities have failed to address fundamental questions about identifying needed capabilities; acquiring them efficiently; and ensuring knowledge and training among both decisionmakers and end users, particularly for conducting influence activities. To gain insights into current and potential practices for acquiring and employing AI for influence-related activities, RAND researchers interviewed experts and conducted a workshop to elicit their tactical and operational needs.



What are influence activities?

"The joint force leverages information to affect the perceptions, attitudes, decision making, and behavior of relevant actors."

(Joint Publication 3-04, *Information in Joint Operations*, 2022, p. ix)

NOTE: *Information operations* is a doctrinally outdated term, so this document instead focuses on *influence activities*.

Who is affected by influence activities?

Relevant actors: "Individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action."

Target audience: "An individual or group selected for influence."

(Joint Publication 3-04, 2022, p. ix and p. IV-25)

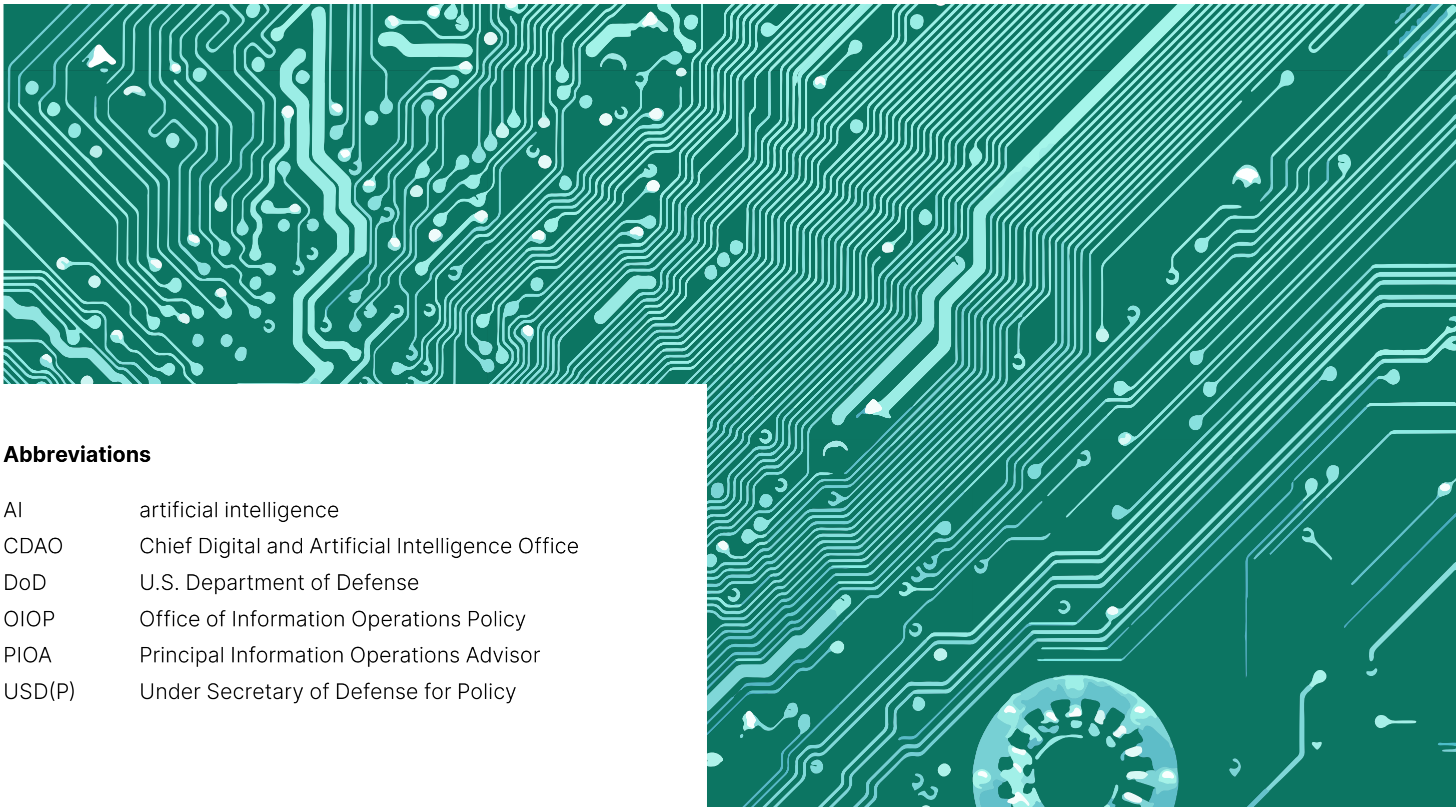
What Is *Influence Activity?*

What is meant by *influence* or *influence activity*? In brief, an *influence activity* is a deliberate attempt to affect a person's or group's thoughts, feelings, or behavior. According to Joint Publication 3-04, *Information in Joint Operations*, published in 2022, "The joint force leverages information to affect the perceptions, attitudes, decision making, and behavior of relevant actors" (p. ix). Joint Publication 3-04 also states, "Relevant actors include individuals, groups, populations, or automated systems whose capabilities or behaviors have the potential to affect the success of a particular campaign, operation, or tactical action" (p. ix). Both Russia and the People's Republic of China are known to have waged recent, prominent influence campaigns against the European Union and the U.S. media using generative AI (with the intent of disseminating disinformation and disrupting elections; see the red box on p. 7, which describes Russia's DoppelGänger campaign and China's Operation Spamouflage). The ability not only to detect and defend against such campaigns but also to mount such campaigns *where appropriate* has made generative AI a critical capability for the military and the Intelligence Community.

Who Directs the Use of AI for Influence Activities?

Title 10, Section 397, of the U.S. Code establishes a Principal Information Operations Advisor (PIOA) to advise the Secretary of Defense on all aspects of information operations within DoD. PIOA oversees policy, strategy, planning, resource management, operations, personnel, and technology for information operations and ensures coordination with the Department of State, the Intelligence Community, and other federal agencies. PIOA also manages risk to prevent U.S. persons from being exposed to information meant for foreign audiences, sets standards for acknowledging operations, and fosters collaboration with the private sector and academia on countering malign influence activities.

In October 2020, the Secretary of Defense designated the Under Secretary of Defense for Policy (USD[P]) as PIOA. To support the assigned responsibilities, the USD(P) formed the Office of Information Operations Policy (OIOP) and established a PIOA cross-functional team with representatives from each of the services. The PIOA cross-functional team studied the *2022 National Defense Strategy of the United States of America* and Joint Publication 3-04



Abbreviations

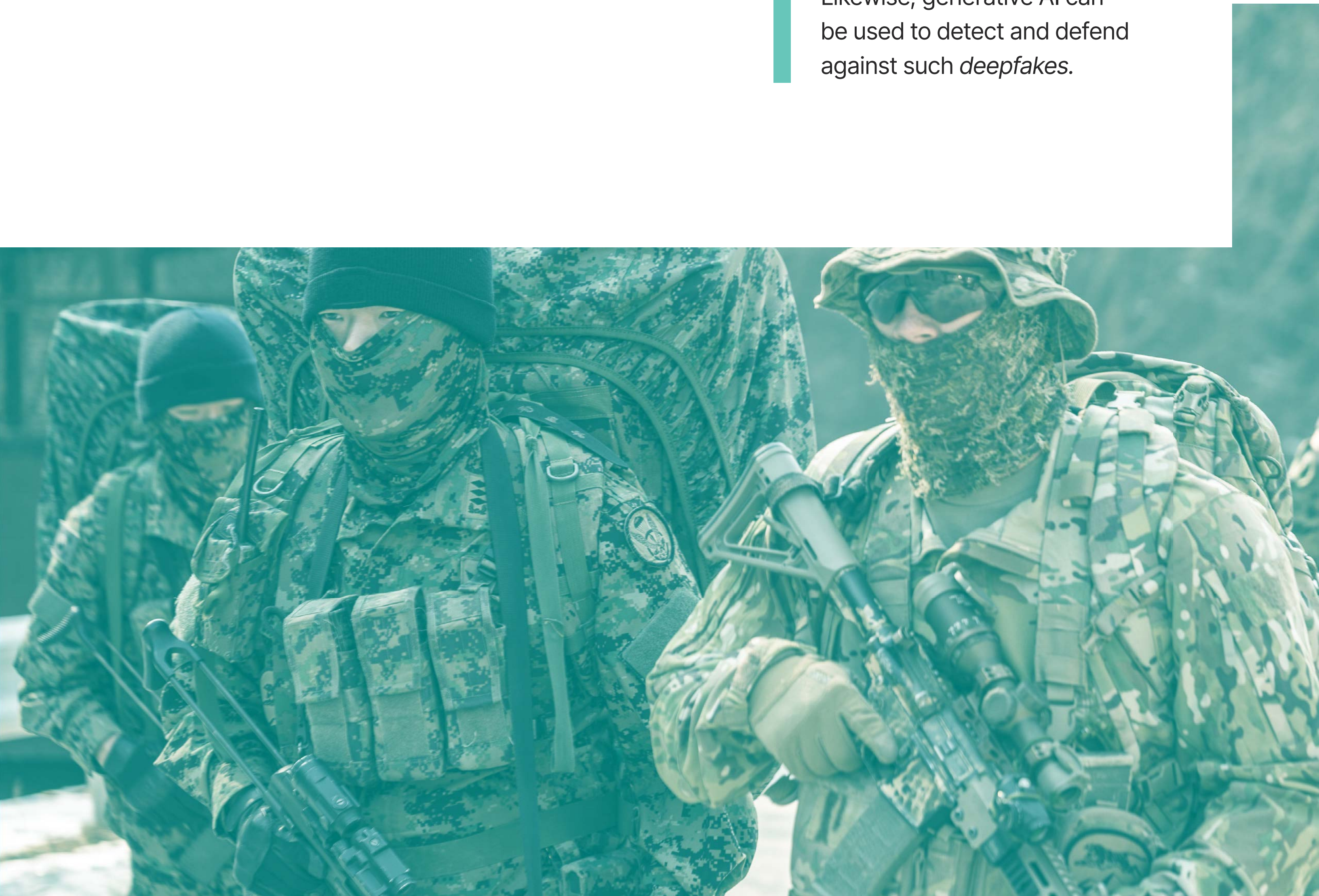
AI	artificial intelligence
CDAO	Chief Digital and Artificial Intelligence Office
DoD	U.S. Department of Defense
OIOP	Office of Information Operations Policy
PIOA	Principal Information Operations Advisor
USD(P)	Under Secretary of Defense for Policy

(*Information in Joint Operations*) and collected inputs from multiple information forces' strategies and foundational documents. The team did this to align the 2023 DoD *Strategy for Operations in the Information Environment* with the 2022 *National Defense Strategy* and focus on building DoD capabilities and capacities to execute operations in the information environment in support of integrated deterrence, campaigning, and building enduring advantages—approaches believed to be needed to advance U.S. national defense priorities and defend and promote national interests.

However, despite these efforts, coordination across the information and influence communities remains challenging—from the lexicon, through bureaucratic roles and responsibilities, to operational execution. This environment does not positively facilitate the provision of clear guidance, prioritization, and resources required for effective, efficient, and dynamic acquisition and development of AI capabilities and tools to conduct influence activities.

What is generative AI, and how is it used in influence activities?

Generative AI is a type of AI that uses models and large databases of textual, visual, and auditory information to create new content. For example, generative AI can be used to create videos that purport to show well-known public figures or members of particular racial or ethnic groups making statements that support or refute particular political viewpoints or committing particular acts. Likewise, generative AI can be used to detect and defend against such *deepfakes*.



What Advantages Does Generative AI Offer Influence Activities?

Generative AI offers information personnel the potential to analyze large volumes of data and to generate high-quality content far more efficiently than with the tools they currently possess. AI-enabled technology does not necessarily introduce novel capabilities but rather force-multiplies a host of existing capabilities. That is, influence professionals already have the capability to craft messages and narratives, conduct audience analyses, counter adversary narratives, and mount their campaigns on social media. But, as noted in a 2023 report by the U.S. Government Accountability Office called *Contested Information Environment: Actions Needed to Strengthen Education and Training for DOD Leaders*, DoD lacks the resources needed to train service members and decisionmakers to operate in the information environment, particularly in an environment of contested information, and the resources needed to manage information. Acquiring AI capabilities for influence is about improving on these capabilities—for example, increasing operational tempo, improving quality (and, thus, influence), and scaling up influence campaigns. But although the potential benefits for adopting generative AI for influence are tremendous, they do not come without risks.

What Are the Uses of AI for Influence Activities, and What Capabilities Can Generative AI Bring to the Table?

In Joint Publication 3-04, the Joint Chiefs of Staff identified three sets of tasks for which they envisioned generative AI playing a role:

- **Understanding how information affects the operational environment:** Characterizing the overall information environment (especially mainstream and social media), identifying the relevant actors, and understanding the range of their potential behaviors
- **Supporting human and automated decisionmaking:** Planning and drafting the desired products, planning operations, and testing messages
- **Leveraging information:** Executing (broadcasting) the products or operations and assessing whether the intended effects were achieved.

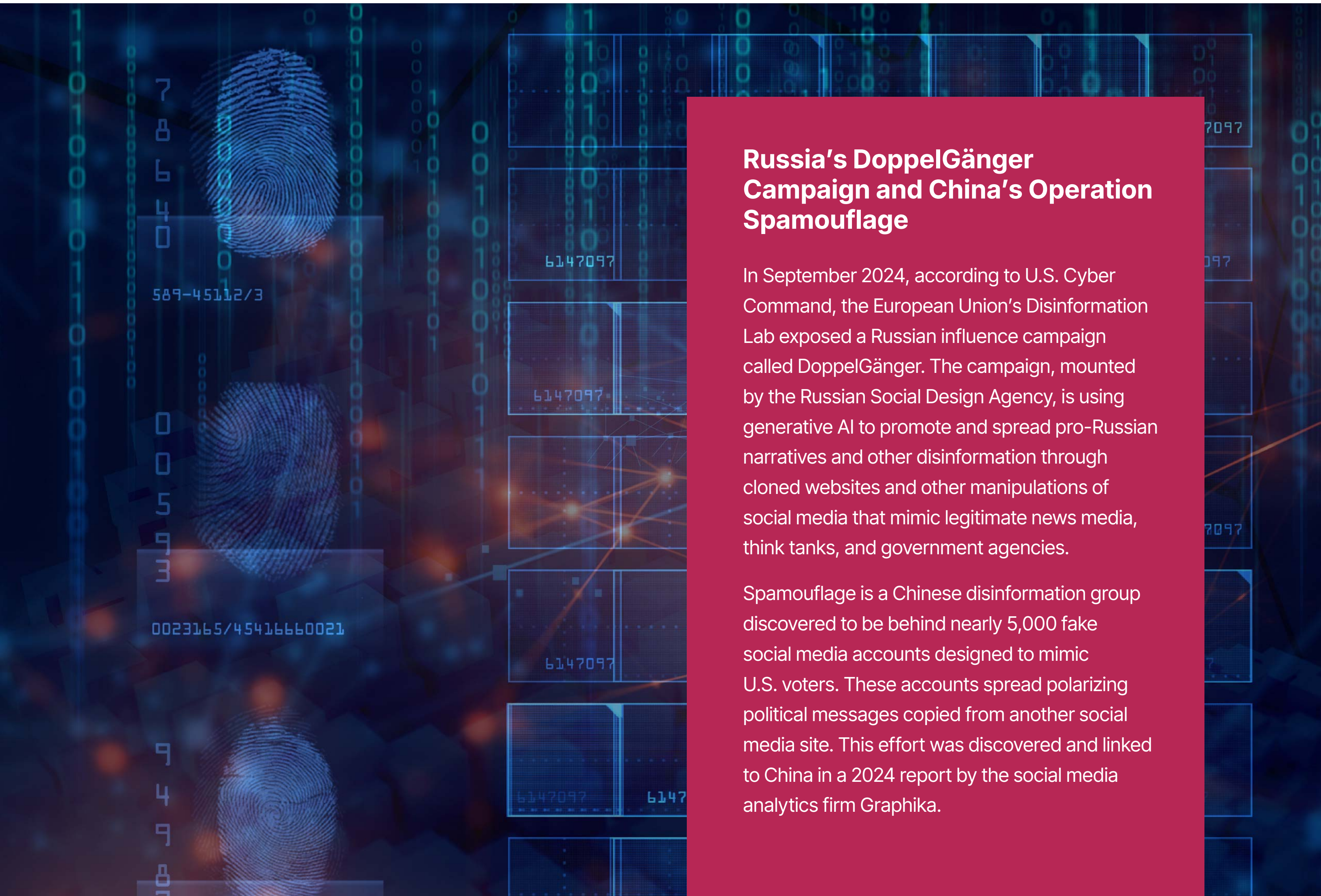
AI can be a vital resource in managing and analyzing the large amounts of data needed to conduct influence operations. Likewise, generative AI can be enormously helpful in creating and disseminating the output of all of that analysis. But these actions require tremendous computing capacity and extensive training of operators and decisionmakers, and both computing and training resources are in short supply (for example, compute requirements have been estimated to have grown four- to fivefold yearly for the past decade).

Acquiring Generative AI and Applying It to Influence Activity Face Risks and Challenges

When DoD considers acquiring generative AI for influence applications, it needs to consider several risks and associated challenges:

- **Technical risks unique to generative AI** include inappropriate model output (called *hallucinations*); the need for expensive hardware, such as graphics processing units; and the challenges of integrating AI into established workflows.
- **Security concerns** include some routine concerns that apply to all software acquisitions but also some that are novel because of the uniqueness of the models and the limited options for assessing vulnerabilities not previously encountered. Also, the repositories of training data need to be protected, so using commercial cloud-based storage is not an option.
- **Adoption risks** include ethical and legal considerations, but they also include being behind the curve of adoption and not having adequate technological skill or literacy.

Not having adequate technological skill or literacy also presents a challenge for identifying the needed capabilities and requirements; acquiring hardware with the needed capacity and the most up-to-date software; establishing processes for verification, validation, testing, and evaluation; and keeping up with rapid technological advances.



Russia's DoppelGänger Campaign and China's Operation Spamouflage

In September 2024, according to U.S. Cyber Command, the European Union's Disinformation Lab exposed a Russian influence campaign called DoppelGänger. The campaign, mounted by the Russian Social Design Agency, is using generative AI to promote and spread pro-Russian narratives and other disinformation through cloned websites and other manipulations of social media that mimic legitimate news media, think tanks, and government agencies.

Spamouflage is a Chinese disinformation group discovered to be behind nearly 5,000 fake social media accounts designed to mimic U.S. voters. These accounts spread polarizing political messages copied from another social media site. This effort was discovered and linked to China in a 2024 report by the social media analytics firm Graphika.

Challenges and Opportunities in Acquiring AI for Influence

DoD has found it challenging for software requirements to be defined and software to be acquired through traditional requirements and acquisition processes for hardware-intensive weapon systems (e.g., aircraft or ships). As a result, DoD has established distinct acquisition pathways and alternative requirements processes for software. But some categories of technologies—such as cyber (computers and other information-related entities) and generative AI—do not conform neatly to the existing acquisition pathways.

Experts identified an array of challenges related to determining the capabilities required for generative AI use in influence operations, acquiring those capabilities, and putting them in the hands of users.

They also offered some suggestions for meeting those challenges (for examples, see Table 1).

Table 1 Key Challenges in Acquiring Generative AI for Influence . . . and Some Possible Solutions

Area	Challenge	Possible Solution
Requirements determination	Communication between acquisition staffs and end users is lacking	Train acquisition professionals and establish open communication with users
Acquisition	No single acquisition pathway fits the needs of generative AI	Tailor existing acquisition pathways to enable needed flexibility
Operations	User training is lacking, and authorities are unclear	Develop tailored training and clear guidance and authorities

To address the challenges presented by generative AI acquisitions, members of the influence community described employing a variety of the available pathways, but each presents its own challenges (see Table 2).

This piecemeal approach to acquisition of generative AI tools and services means that the influence community never develops the road map or architecture that developers, acquirers, and operators need to adhere to for a coordinated effort and to conduct operations at scale. And beyond initial acquisition, sustainment efforts would greatly benefit from a coordinated strategy across organizations performing influence. In 2023, with this in mind, DoD released its *Data, Analytics, and Artificial Intelligence Adoption Strategy*, which provides a framework for determining the appropriateness of acquiring shared AI. This

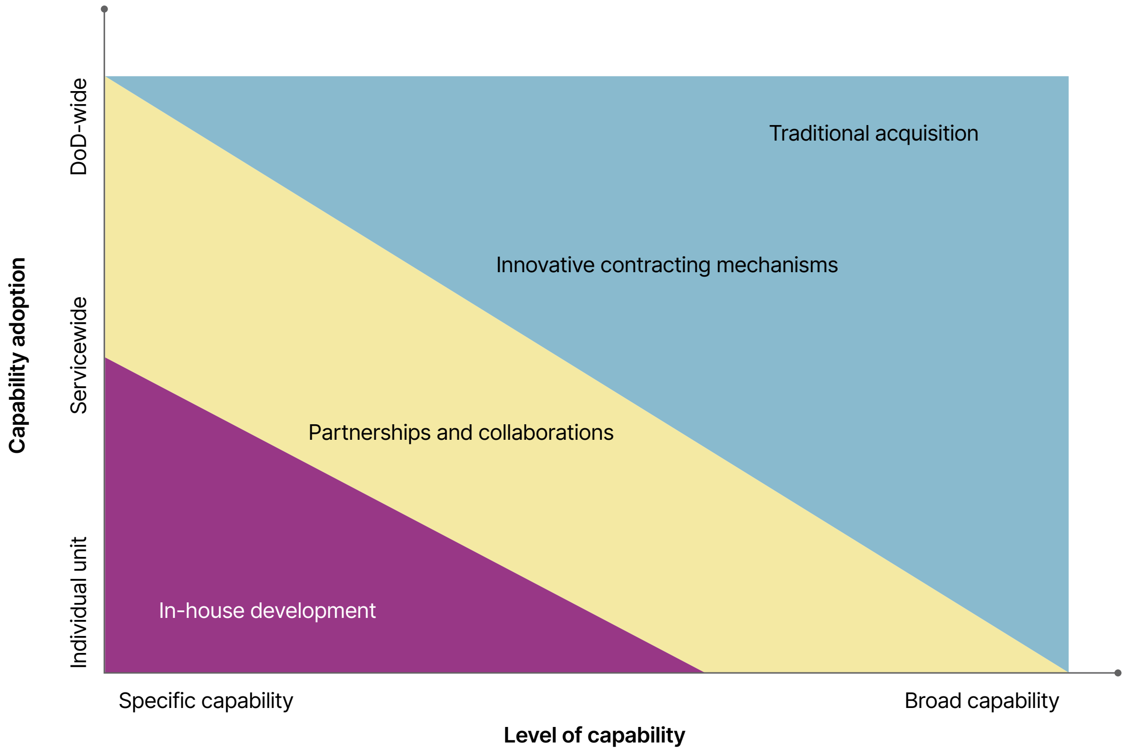
Table 2 Approaches Being Used to Acquire Generative AI

Approach	Description	Advantages	Challenges
Software acquisition pathway	Emphasizes iterative development and continuous delivery	Adapts to changing requirements more easily than do traditional approaches	Is still time-consuming and requires program management structure
Innovative contracting mechanisms (e.g., Other Transaction Authority)	Are exempt from several federal contract regulations and reporting requirements	Facilitate collaboration with nontraditional vendors	Can lead to less transparency Can be difficult to transition to a traditional contract mechanism or a program of record
Partnerships	Are based on collaboration with experts to identify, procure, and sustain needed capabilities	Leverage expert knowledge Ease transition from prototype to fielded capabilities	Require alignment of priorities with external stakeholders Can require unacceptable sharing of intellectual property and data rights
Purchase and in-house modification or development	Uses operation and maintenance funds to purchase commercial off-the-shelf tools or services	Allows quick purchases with shorter approval chain	Encourages redundant purchases Often involves yearly contracts that require renewal

framework (a simplified version of what is shown in Figure 1) considers the trade-offs between the complexity of implementing a particular AI tool and the similarity of intended outcomes across organizations to steer the selection of a shared or centralized AI tool versus a bespoke AI tool.

Within the framework, an AI tool can be identified along a level of capability (horizontal axis), from specific to the influence community to generalizable across the broader defense community. An AI tool can also be identified along a scale of capability adoption (vertical axis) as adopted by an individual unit or more broadly adopted by all of DoD. Where a tool falls along these spectra can help determine how that tool is most appropriately acquired. Broadly applicable tools that large portions of DoD adopt, such as ChatGPT, should be procured and maintained broadly by DoD or the Chief Digital and Artificial Intelligence Office (CDAO). In contrast, tools that are specific to the influence mission, such as the Army's Ghost Machine, should be acquired by an individual unit or organization. (Ghost Machine is a tool developed by the U.S. Army that enables operators to use inexpensive, accessible technology for deception by mimicking, targeting, and influencing enemy soldiers.)

Figure 1 Generative AI Applicability and Acquisition Framework



Recommendations

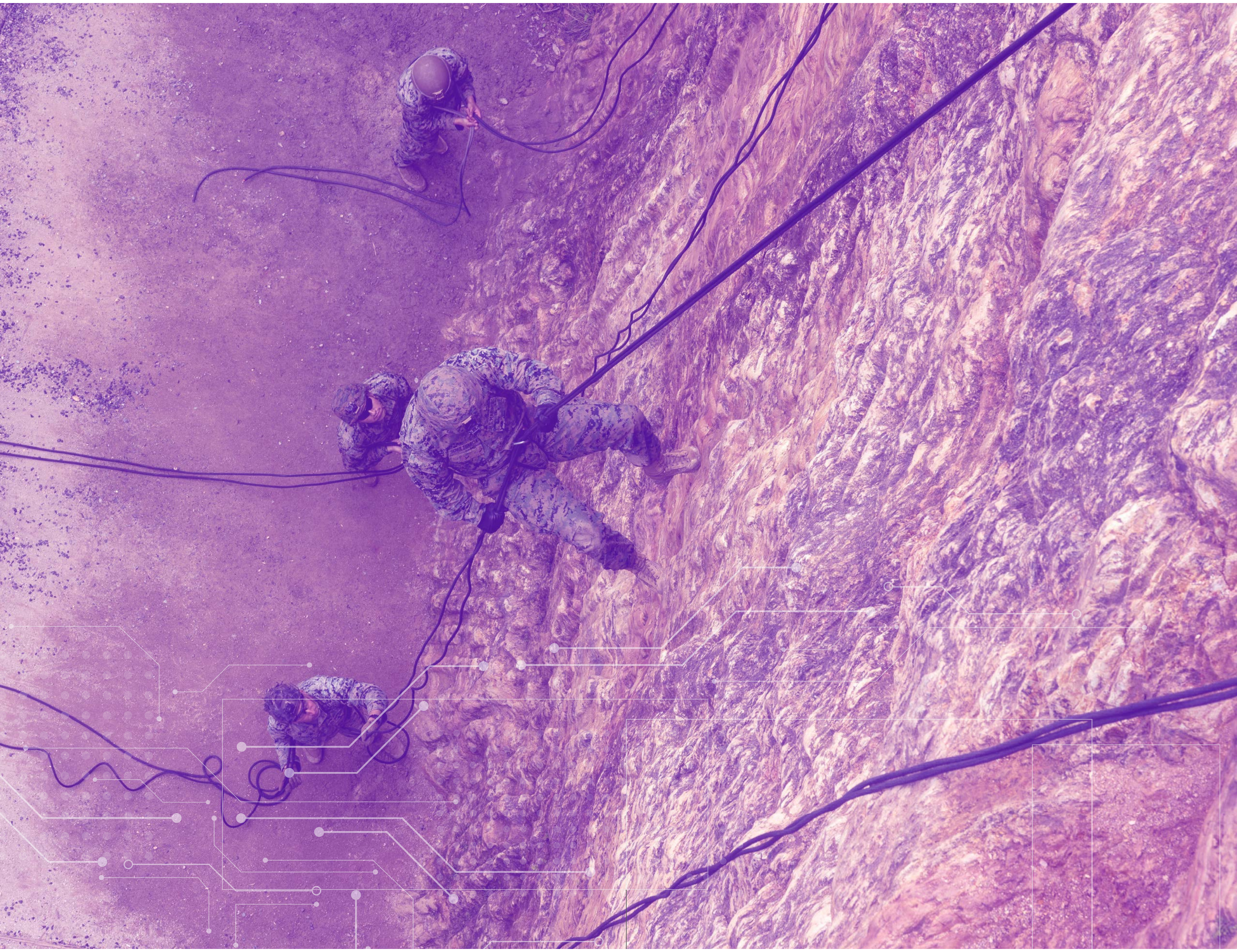
In any discussion of influence activities, much of the attention tends to focus on policy issues, such as ethical boundaries, rather than on the administrative and technical challenges and barriers. The concerns raised by the experts and members of the influence community alike suggested a series of recommended steps that, if implemented, will help overcome the challenges and guide this work in a positive direction (see Table 3).

Conclusions

This research underscores the critical role of generative AI in enhancing DoD's influence activities in both competition and conflict. The complexities and scale of strategic competition necessitate advanced AI capabilities to process and analyze large volumes of information, create tailored content, and ultimately maintain an operational edge. Generative AI can improve analysis, operational planning, and assessment of influence activities. But it presents a tool, not the answer, and maximizing its potential will take dedicated effort in several areas. Relying on legacy acquisition systems to build this capability incurs risk that DoD cannot afford. As DoD expands and accelerates its acquisition approaches for software, it must also consider the unique requirements of AI acquisition.

Table 3 DoD Acquisition of AI for Influence Activities: Findings and Recommendations

Area	Findings	Recommendations
Influence	**Currently, acquisition of generative AI for influence activities is characterized by lack of investment and disunity of effort.** Although the importance of influence is acknowledged, its definition and the roles of DoD stakeholders are unclear, resulting in insufficient prioritization within the joint information function. This lack of coordination leads to varied tasks across echelons and contributes to procurement inefficiencies.	PIOA should direct OIOP to enhance collaboration within the influence community. The military services and U.S. Special Operations Command should prioritize the acquisition of generative AI. It is essential to define influence activity requirements, encourage investment, foster stakeholder collaboration, and coordinate with DoD AI agencies for common infrastructure.
Acquisition	**Effective acquisition requires a strategic and flexible approach *and* a sustainment process that addresses both enterprise and bespoke capabilities.** Multiple pathways are needed to address diverse requirements and emerging capabilities, yet few incentives drive developers to enhance existing tools. The lack of standardized assessment criteria for generative AI tools, combined with acquisition professionals' limited technical expertise, complicates the procurement of this rapidly evolving technology.	The services should identify suitable organizations to manage AI acquisition and leverage available strategies for flexibility across AI capabilities. A formal process to define generative AI requirements is essential, along with developing sustainment strategies and increasing the tempo for capability purchases.
Technology	**No enterprisewide plan addresses generative AI implications for influence activities.** DoD's technology acquisition has prioritized data and AI, yet limited training and resources hinder decisionmakers' understanding of AI as an influence enabler. This shortfall also affects the potential for improved interoperability with allies and partners.	PIOA and OIOP should identify and invest in training and education opportunities while developing guidelines to govern the use of AI-generated outputs in influence activities, ensuring effective and efficient adoption.



This research summary describes work done in the RAND National Security Research Division and documented in *Acquiring Generative Artificial Intelligence to Improve U.S. Department of Defense Influence Activities*, by William Marcellino, Jonathan Welch, Brittany Clayton, Stephen Webber, and Thomas Goode, RR-A3157-1, 2025 (available at www.rand.org/t/RRA3157-1). To view this research summary online, visit www.rand.org/t/RBA3157-1. RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

Photo credits: Front cover: Matt Britton/U.S. Army; p. 2: Mary Torres/U.S. Marines; p. 5: Seonghyeon Bae/U.S. Army; back cover: JVonnta Taylor/U.S. Marines.

www.rand.org

RB-A3157-1