The Eisenhower School for

National Security and Resource Strategy

13

AY 2024-2025

THE CYBER IMPERATIVE: HOW BUREAUCRACY AND INERTIA THREATEN AMERICA'S CYBER EDGE

Information and Cyberspace Industry Study Group Paper

Dr. James Van de Velde

Co-Authored By: Seminar 7

WORD COUNT: 8246

May 15, 2025

The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Table of Contents

Seminar 7 Students and Faculty

Students

LTC Catherine Carlson, U.S. Army

LTC Erich Feige, U.S. Army Reserve

LTC Georgios Frangou, Cyprus Army

Col Colin Hanson, U.S. Air Force

LtCol Blake Jackson, U.S. Marine Corps

Ms. Nicole Jackson, Department of the Air Force

Col Buckley Kozlowski, U.S. Air Force

CDR Kathryn Moretti, U.S. Coast Guard

Mr. Samuel Peale, Department of State

Ms. Debra Porter, Department of the Army

Lt Col Scott Roberts, U.S. Space Force

COL Joel Smith, U.S. Army

Mr. Jeffrey Weinshenker, Department of State

BG Riadh Zaibet, Tunisian Army

Faculty

Dr. James Van de Velde, Ph.D., Industry Study Lead

CAPT Robert Goad, Industry Study Deputy, U.S. Navy

Field Studies Hosts and Guest Speakers

Academia

1. Professor Jennifer Golbeck, University of Maryland, *Social Engineering*
2. Dr. Dana Young, University of Delaware, *The Demand Side of Mis/Disinformation*
3. Professor Dan Silverman, Carnegie Mellon, *Seeing is Disbelieving*

Industry

4. Dr. Lindsay Hundley and Dr. Ingrid Dickenson, Meta Security Policy, *Misformation and Cyber-Espionage*
5. Ylli Bajraktari, President and CEO, Special Competitive Studies Project (SCSP)
6. Grant Smith, Business Development Director, CLEAR, Thompson Reuters Special Services, *Open Source Data Analysis and Supply Chain Security*
7. Hari Ravi, Photon Insights, *Machine Learning Applications, Securing AI and the Future of LLMs*

Government/NDU President's Lecture Series

8. Gen Timothy Haugh, Commander USCYBERCOM, *Overview of USCYBERCOM and NSA*
9. LtCol Aaron Rosenblatt, Future Plans JFHQ-DODIN, *DODIN Architecture, Cybersecurity, and Roles and Responsibilities*
10. Mr. Rob Joyce, NSA Director of Cybersecurity
11. Mr. Paul Mazzucco, USCYBERCOM J5,
12. Mr. Dylan Presman, White House Office of National Cyber Director, *Cyber Security Issues and Policy*

Washington D.C. Couplet

13. Geoff Brown, Chief of Strategic and External Communications, Johns-Hopkins University Applied Physics Laboratory, *Advanced Research Projects Including Robotics, AI, and Human-Machine Integration*
14. Tac-Link, *Tech Industry Venture Capital, and Public Outreach*
15. Yelena Osipova-Stocker, Strategic Analyst, Office of Policy and Research, U.S. Agency for Global Media, *Overview of USAGM and Current Programs; Tour of USAGM and VOA*
16. Roman Napoli, Acting USAGM CEO
17. Mwaymo Hamza, Africa Division, Voice of America
18. Mark, V. Zimmer, Director, Counter-Terrorism Division, Department of State, Counter Foreign Information Manipulation & Interference, *Countering Foreign Malign Influence*

New York City Couplet

19. NASDAQ, Ms. Lee Anne Milhiser, *Financial Sector Cybersecurity Operations*
20. Fordham University, Gabelli School of Business, *The Business of Cybersecurity*
21. FBI NY Field Office Cyber Division, Special Agent George Tsang, *Chinese, and DPRK Persistent Threats*
22. The NYC Office of Technology & Innovation, NYC Cyber Command, *Overview of NY CYBERCOM Operations and Threats*
23. The Paley Center for Media, Mr. Carloa Pareja, *History of Political Advertisements*
24. CISA, Nicholas Zink Outreach Coordinator, *Protecting Critical Infrastructure*

Silicon Valley, California

25. HP, Dr. Tommy Gardner, Chief Technology Officer, *Overview of HP AI Research, Development and Applications.*
26. Lawrence Livermore National Labs (LLNL), Reg Beer, *Lab Overview*
27. Apple (former executive), Mr. Jon McCormick, *Perspectives on AI*
28. Oracle, Eric Sedlar, Vice President and Tech Director, *Could Platform and Applications*
29. NVIDIA, Kevin Berce, Govt. Affairs Team, Engineering Staff, *AI Applications and Hardware Design*
30. IBM, Christina Howell, *Overview of IBM*; Spike Narayan, *IBM Research*; John Arther, *North Pole*; Sandeep Gopisetty, *Watsonx*; Kevin Roche, *Quantum Computing*
31. Google Cloud Space, Juan Quinones, *Google Security*; Alice Friend, *Cyber-Security Policy*; Justin Webb; Courtney Chapman
32. In-Q-Tel, AJ Bertone Managing Partner, *Overview of In-Q-Tel*
33. Defense Innovation Unit (DIU), Cullen Greenfield CDR USN, *Overview of DIU and Major Projects*
34. Shield Capital, Mr. Mike Brown Partner, *Tech Industry Outlook and Venture Capital Strategies*
35. DCVC, Matt Ocko, Co-Founder, Co-Managing Partner, *Private Sector Role in National Security*

Tokyo, Japan

36. U.S. Embassy, Charge, and Country Team, *Embassy Brief and Overview of Japanese Space and Cyber Industries and Cooperation*; Gloria Glaubman, DoS Cyber
37. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Director General Kimihko Kimura and Mr. Tanoki Sano, *Implementing Japan's Active Cyber Defense Strategy*
38. National Police Agency Cyber Affairs Bureau, Hiroaki Hirayama, *Implementing Japan's Active Cyber Defense Strategy*
39. JPCERT, Dr. Koichiro Komiyama, CISSP Director, *Public-Private Partnerships in Cyber-Security*
40. Ministry of Defense, Cyber Buildup and Planning Division, Ms. Ayako Sakata, *Japanese Defense Force Cyber Capabilities*; Tour of SDF CYBERCOM
41. National Security Secretariat, Mr. Keisuke Kodama, *National Security Strategy of Japan*
42. Senior Advisor to the Cabinet and Former National Security Advisor to the Prime Minister, Mr. Takeo Akiba, *Japanese National Security Policy*
43. NTT, Ms. Mihoko Matsubara, Chief Cyber-Security Strategist, *Cyber-Security Strategy and Policy*
44. NEC, Mr. Fukushima, *NEC Creation Lab, and Security Technologies*
45. FUJITSU Laboratories, Mr. Yashima Kaita, *Fujitsu Research and Role in Japan's DIB*

Hawaii

46. USINDOPACOM, J2/J8, *USINDOPACOM Cyber Threat Overview and Counter-China Strategy*; *COIPE, USCYBERCOM Support to USINDOPACOM*
47. Asia Pacific Center for Security Studies, Dr. Inez Miyamoto, *Back-Brief of Japan Field Study*

Executive Summary

To maintain national security in a complex information and cyberspace landscape, the United States must execute decisive policy reforms that invest in innovative technologies, build digital supply chain resilience, develop the cyber workforce, and secure the advantage in the information domain. Unless the United States radically changes its approach through bold policy reform, it risks ceding the digital battlespace entirely.

This paper applies a four-part operational framework to assess America's vulnerabilities and prescribe actionable reforms. The framework focuses on four Lines of Effort (LOEs): regulating and scaling innovative security solutions, building digital supply chain resilience, developing a future-ready cyber workforce, and securing informational advantage.

Key Findings:

Innovation vs. Inertia: While the private sector races ahead in AI and cybersecurity innovation, DoD systems lag due to antiquated procurement processes and ineffective regulation. Weak regulatory enforcement and segmented security architecture compound these issues.

Digital Supply Chain Fragility: The defense industrial base suffers from fragmentation, poor interoperability, and overreliance on foreign suppliers, particularly from China, posing systemic cybersecurity and logistics risks.

Cyber Talent Shortfall: With over 450,000 cybersecurity vacancies and a hiring system mired in red tape, the U.S. cannot meet workforce demands. Outdated hiring policies and poor retention hinder the government from competing with the private sector.

Information Environment Under Siege: Disinformation, censorship, and algorithmic manipulation exploit regulatory loopholes, erode public trust, and allow adversaries—especially China—to shape global narratives at the expense of democratic values.

Recommendations:

Institutional Reform: Adopt a "Three Layers of Cyber Defense" model, implement integration readiness levels, and elevate technology adoption across DoD and federal agencies as a core leadership metric.

Supply Chain Modernization: Create a National Digital Supply Chain Security Council, enforce dynamic certification models, and mandate zero-trust architecture across the defense ecosystem.

Workforce Development: Establish a Cyber Reserve Force, modernize federal hiring, and expand K-12 and postsecondary cybersecurity education through public-private partnerships.

Informational Advantage: Update legal frameworks, expand media literacy education, and launch targeted strategies to counter foreign censorship, especially China's influence over U.S. tech and media.

Conclusion:

Technical tools alone cannot close America's cyber gap. Decisive policy action across government, industry, and civil society is necessary to overcome systemic inertia and protect national interests. This paper offers a strategic roadmap prioritizing adaptability, public-private collaboration, and enduring resilience. By acting with urgency and unity, the United States can reclaim its edge in cyberspace and defend the principles that underpin its global leadership.

The first major cyber-attack on the internet did not originate from a state-sponsored threat actor, a criminal organization seeking financial rewards, or a hacktivist seeking to fulfill an ideological agenda. It happened in 1988 when a PhD student at Cornell University ran a scientific experiment to see how many computers he could infect. Robert Morris Jr.'s worm didn't just cripple the Cornell network; it proliferated at a remarkable speed and, within 24 hours, affected approximately 10% of global computers connected to the internet. Though the worm did not damage or destroy files, it slowed computers to a crawl, impacting national security and research and development at elite universities and national laboratories.[1] The Morris Worm marked the beginning of the growth in complexity and vulnerabilities in the information and cyber domain.

Introduction

To maintain national security in a complex information and cyberspace landscape, the United States must execute decisive policy reforms that invest in innovative technologies, build digital supply chain resilience, develop the cyber workforce, and secure the advantage in the information domain. Unless the United States radically changes its approach through bold policy reform, it risks ceding the digital battlespace entirely.

Today, an explosion of advanced persistent threats (APTs), ransomware gangs, and insider threats characterize the information and cyberspace domain at an unprecedented scale and level of sophistication. Despite decades of investment, the United States is losing its competitive advantage in the cyber and information domains because of its outdated laws, bureaucratic silos, and institutional fear of escalation. While adversaries like China and Russia act with speed and cohesion, America dithers. Its cyber defenses are reactive, fragmented, and often misaligned with the tempo of modern threats.

Moreover, senior leaders must consider the nexus between cyber and the broader information environment. The rapidly evolving traditional media landscape, ubiquity of social networks, and destructive spread of disinformation, information warfare, and authoritarian censorship represent a parallel sphere of great power competition that overlays onto the cyber domain. To succeed in

the broader digital domain, the United States must aggressively shape this information ecosystem to its advantage.

This paper will assess the strategic environment and stakeholders in the cyber and information space. It will then analyze these industries along four distinct lines of effort (LOEs). The resulting recommendations will strengthen America's ability to set the pace of worldwide cyber and information operations.

Strategic Environment

The information and cyberspace strategic environment is marked by rapidly evolving global competition.[1] In the United States, rapid innovation, supply chain vulnerabilities, an inadequate workforce, and information challenges present both opportunities and risks.[2] Abroad, state and non-state actors aggressively use cyber technology to disrupt productivity and influence the American population.[3]

United States Domestic Environment

The digital domain is uniquely challenging because the private sector operates a significant portion of cyberspace. Large corporations own and operate the most critical infrastructure, from telecommunications networks and financial services to energy, chemicals, and manufacturing. Meanwhile, technology platforms like Meta, Google, and Amazon have amassed more power

[1] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025.
[2] International Information System Security Certification Consortium (ISC)², *2023 Cybersecurity Workforce Study*, accessed April 20, 2025, https://www.isc2.org/Research/Workforce-Study; Edelman, "2025 Edelman Trust Barometer," accessed April 17, 2025, https://www.edelman.com/trust/2025/trust-barometer; Blake Jackson, "The Digital Defense Industrial Base: Ensuring Secure and Agile Logistics Networks" (Individual Paper, AY 2024-2025).
[3] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025.

and influence than many nation-states.[4] Though dominated by the private sector, advances in cyberspace technology and corresponding policy have implications for multiple government sectors. Similarly, cyber infrastructure touches almost all industries, even those unrelated to the cyber field. Thus, cyber policies have consequences for all facets of American society.

Recent guidance has acknowledged the importance of the cyber domain. The National Cybersecurity Strategy (2023), National Defense Strategy (2022), and National Security Strategy (2022) emphasize the necessity of public-private partnerships, resilient infrastructure, coordinated interagency efforts, and international cooperation.[5] Initiatives like the CHIPS and Science Act and the Inflation Reduction Act integrate cybersecurity into broader national economic and infrastructure initiatives.[6]

While the introduction of cyber and security guidance into United States strategy represents progress, the lack of an overarching body ensuring unity of effort creates challenges for policy implementation. Stove-piped regulatory organizations result in misaligned authorities, inadequate cross-sector coordination, and systemic vulnerabilities.[7] Existing legal, ethical, and regulatory frameworks are insufficient and assume increasing risk to the public and private sectors.

The commercial cybersecurity sector is rapidly innovating the deployment of artificial intelligence, cloud computing architectures, and automated threat detection systems. [8] Technology giants like Microsoft, Google, and Amazon use machine learning to enhance

[4] Ian Bremmer, "How Big Tech Will Reshape the Global Order," *Foreign Affairs*, November/December 2021, https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order.
[5] Office of the National Cyber Director, *National Cybersecurity Strategy*, March 2023.
[6] CHIPS Act of 2022, Pub. L. No. 117-167, 136 Stat. 1392 (2022).
[7] National Security Commission on Artificial Intelligence, *Final Report*, March 2021.
[8] KPMG, "Cybersecurity Considerations 2024: Government and Public Sector," KPMG Insights, accessed April 2, 2024, https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2024-government-and-public-sector.html.

anomaly detection, predict intrusions, and automate responses.[9] Venture-backed startups are innovating zero-trust network access, endpoint detection and response, and continuous security validation.[10] These developments have enabled private firms to respond to threats quickly and precisely.[11]

The federal government and defense sectors are not keeping pace with these advances.[12] Many Department of Defense (DoD) systems operate on legacy architectures that are either insecure or incompatible with modern cybersecurity tools.[13] This issue is compounded by slow acquisition cycles and risk-averse procurement strategies that hinder the rapid integration of emerging technologies.[14]

Furthermore, the American defense industrial base (DIB) now operates within a complex, digitized environment, with a lack of transparency and a reliance on fragmented global networks.[15] The disaggregation that decreased costs now presents a cyber risk to suppliers at all levels of the DIB. Even when protective measures are clearly defined, many manufacturers lack the means to implement them. Small and mid-sized companies often lack the human and

[9] Jenna Phipps, "Top 20 Cybersecurity Companies You Need to Know in 2025," eSecurity Planet, March 21, 2025; Cybersecurity Profile: AWS Ground Station Network (n.d.); Azure Orbital Ground Station: Mission-Orientation and Cyber-Security Posture Assessment (n.d.).
[10] Ibid
[11] Fnu Jimmy, "The Role of Artificial Intelligence in Predicting Cyber Threats," International Journal of Scientific Research and Management 11, no. 8 (2023); Deloitte, Stellar safeguards: How organizations can protect space assets from cyber threats, August 29, 2024.
[12] Scott Roberts, "From Compliance to Resilience: Strengthening United States Space Force Ground System Cybersecurity" (Individual Paper, AY 2024-2025); National Security Commission on Artificial Intelligence, *Final Report*, March 2021.
[13] U.S. Space Force Cybersecurity Profile: A Mission-Oriented vs. Compliance-Driven Assessment (MOI/CSP Framework) (n.d.).
[14] Shahzad et al., "Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers," Systems 12, no. 10 (2024); National Security Commission on Artificial Intelligence, *Final Report*, March 2021.
[15] Izabela Rojek et al., "Review of the 6G-Based Supply Chain Management within Industry 4.0/5.0 Paradigm," Electronics 13, no. 13 (July 4, 2024).

financial resources to meet baseline cybersecurity standards, making them vulnerable targets and weak links in DoD supply chain security.[16]

The increasing scope and sophistication of cyber threats demand more skilled professionals able to adapt to rapidly changing technologies.[17] The United States faces a persistent shortage of cyber professionals, posing serious consequences for national competitiveness and strategic stability as adversaries utilize cyber capabilities to gain asymmetric advantages.[18]

The CHIPS and Science Act of 2022, often noted for its emphasis on semiconductor production, contains key provisions supporting cybersecurity workforce development.[19] These include increased funding for STEM education, investment in regional innovation hubs, and grants for workforce training. The Act's multi-sector approach encourages government, academia, and industry collaboration, framing cybersecurity workforce development as an integral component of national competitiveness.[20]

While the American private sector leads cyber innovation, the United States government has failed to enact policy to protect its infrastructure, creating defense supply chain risks. Initial efforts are underway to increase protective measures and bolster the workforce. However, they are hampered by a lack of coordination and unity of effort.

---

[16] ChatGPT, response to "Explain cybersecurity risks in digital defense logistics and define the cyber poverty line," April 20, 2025, OpenAI; "Study Suggests Only 4% of DoD Contractors Are Ready for CMMC," Greenberg Traurig, October 2024.

[17] Bureau of Labor Statistics, "Information Security Analysts," accessed March 19, 2025, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

[18] International Information System Security Certification Consortium (ISC)², *2023 Cybersecurity Workforce Study*, accessed April 20, 2025, https://www.isc2.org/Research/Workforce-Study; Lauren Feiner, "Chinese Hackers Outnumber FBI Cyber Staff 50 to 1, Director Wray Says," CNBC, April 28, 2023, https://www.cnbc.com/2023/04/28/chinese-hackers-outnumber-fbi-cyber-staff-50-to-1-director-wray-says.html.

[19] CHIPS Act of 2022, Pub. L. No. 117-167, 136 Stat. 1392 (2022).

[20] Ibid

International Environment

The international cyber environment is characterized by state and non-state actors attempting to capitalize on gaps in American cyber capabilities by conducting cyber operations for disruption, espionage, influence campaigns, and strategic advantage.[21]

China and Russia aggressively target vital infrastructure, conduct economic espionage, and engage in intellectual property theft.[22] These autocratic states exert stringent control over digital spaces and exploit cyber capabilities to suppress dissent and expand geo-political influence.[23] The proliferation of artificial intelligence (AI) aids these efforts by exacerbating strategic competition, reducing barriers to military applications, and increasing risks of destabilization and unintended escalation.[24]

Iran and North Korea further complicate this landscape through disruptive cyberattacks targeting the United States and its allies.[25] Additionally, non-state actors, such as criminal networks and state-supported APTs, exploit vulnerabilities to compromise critical systems, steal sensitive information, and conduct sustained clandestine activities.[26]

---

[21] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025.

[22] Gatestone Institute, China's Cyber War Against America, accessed April 19, 2025, https://www.gatestoneinstitute.org/19569/china-cyber-war-america; Department of Defense Chief Information Officer, *Defense Industrial Base Cybersecurity Strategy*, accessed April 19, 2025, https://dodcio.defense.gov/Portals/0/Documents/Library/DIB-CS-Strategy.pdf.

[23] "Beijing's Global Megaphone," Freedom House, accessed March 26, 2025, https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone; Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability," Perspectives on Politics 13, no. 1 (March 2015).

[24] Artificial General Intelligence's Five Hard National Security Problems (RAND Corporation, February 10, 2025); "Artificial Intelligence, International Competition, and the Balance of Power" (TNSR, May 15, 2018).

[25] Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, March 2025; Joe Tidy, "North Korean Hackers Cash out Hundreds of Millions from $1.5bn ByBit Hack" (British Broadcasting Corporation, March 9, 2025), https://www.bbc.com/news/articles/c2kgndwwd7lo.

[26] The Hacker News, "Google: Over 57% of Nation-State Threat Actors Use Generative Al for Cyber Attacks," January 30, 2025, https://thehackernews.com/2025/01/google-over-57-nation-state-threat.html; Maria Valentina Clavijo Mesa, Carmen Elena Patino-Rodriguez, and Fernando Jesus Guevara Carazas, "Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains," Information 15, no. 11 (2024).

Efforts at international cooperation to counter such threats are hampered by conflicting priorities and threat assessments.[27] Nations prioritizing domestic political agendas fragment international cybersecurity cooperation and weaken collective defense mechanisms.[28] Misinformation campaigns and targeted digital manipulation significantly amplify these risks, eroding public trust, deepening societal divisions, and complicating unified responses to cybersecurity threats.[29]

Stakeholder Interests

Cybersecurity in the 21st century is a shared responsibility among government, industry, and private citizens, each with distinct but interconnected interests. As digital systems underpin nearly every aspect of modern life, protecting them has become essential to national security, economic stability, and public trust. The evolving information environment, marked by disinformation, surveillance concerns, and rapid technological change, further complicates this landscape. Understanding stakeholder priorities is key to developing effective strategies that strengthen the digital ecosystem while preserving democratic values. The following synthesis explores how each group engages with and benefits from a more secure and resilient cyber domain.

Government Interests

Government interests in cybersecurity are anchored in national defense, public safety, and infrastructure security. Federal agencies such as Cyberspace and Infrastructure Security Agency

[27] Debra Porter, "International Artificial Intelligence in Defense and Dual-Use Applications: Accelerating Innovation, Reshaping Industry, And Navigating Security Challenges" (Individual Paper, AY 2024-2025).
[28] "National Security Strategy of Japan (Provisional Translation)," Japanese National Security Council, December 16, 2022, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf; The 1856 Paris Declaration.
[29] "2025 Edelman Trust Barometer," Edelman, accessed April 17, 2025, https://www.edelman.com/trust/2025/trust-barometer); Joel Smith, "Openness V. Censorship: How The Information Industry Can Support Democracies Against A Pandemic Of False Information" (Individual Paper, AY 2024-2025); Craig H. Allen Jr., "The Coast Guard Must Prepare for Al-Enhanced Disinformation," U.S. Naval Institute, June 1, 2024, https://www.usni.org/magazines/proceedings/2024/june/coast-guard-must-prepare-ai-enhanced-disinformation.

(CISA), DoD, NSA, and DHS lead the charge, implementing policies and partnerships that reinforce cybersecurity posture across sectors. Legislative tools like the CHIPS and Science Act and Executive Orders provide funding and regulatory frameworks to drive innovation and secure critical infrastructure.[30] These efforts indicate that cybersecurity is no longer a merely technical concern, but a strategic imperative tied directly to national power projection and economic stability.

Government stakeholder mobilization involves enhancing internal capacity through workforce development, such as expanded cyber education pipelines and reduced reliance on external contractors. The National Initiative for Cybersecurity Education (NICE) and the concept of a Cyber Reserve Force aim to surge capabilities in crisis and provide sustained readiness.[31] Additionally, public-private partnerships (e.g., JCDC, CITEP) are essential to accessing private-sector expertise and bridging visibility gaps in proprietary systems.

The United States government has a strategic imperative to safeguard the information environment and combat adversarial state influence. Any attempts at policymaking or regulation must balance public confidence in the integrity and trustworthiness of information with the need to avoid perceptions of state censorship. Public-private collaboration is essential to achieving this balance and to engaging mass audiences on media literacy and the responsible use of social media and information technology.

Industry Interests

Industry is driven by the need to protect intellectual property, ensure business continuity, and sustain competitive advantage. Cybersecurity is fundamental to these objectives, particularly

[30] CHIPS Act of 2022, Pub. L. No. 117-167 136 STAT. 1367, 394 (2022). https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.
[31] "The NICE Cybersecurity Workforce Framework Explained - Tech Talent Partners - Procom," September 13, 2024. https://procomservices.com/en-us/the-nice-cybersecurity-workforce-framework-explained/.

within national defense and critical infrastructure sectors. The DIB illustrates the dual role of supporting national security while advancing market competitiveness. Firms benefit from government collaboration through stable contracting, access to threat intelligence, and expanded market opportunities via joint innovation programs like In-Q-Tel and the Defense Innovation Unit (DIU).[32]

Industry mobilization includes adopting standardized security frameworks (e.g., CMMC, NIST), participating in joint threat exercises, and investing in automation, AI, and predictive analytics to enhance defense posture.[33] While larger firms face fewer hurdles in meeting regulatory compliance requirements, government support for small and medium-sized businesses is necessary to ensure supply chain resilience.[34] The industry also plays a key role in workforce development, advocating for skills-based hiring, immigration reform, and apprenticeship models to close talent gaps.

In the information domain, traditional news media and corporate stakeholders, from movie studios to big tech platforms, serve as influential platforms of American soft power. However, they face tremendous pressure from authoritarian regimes like China to comply with censorship demands.[35] While these industries broadly support United States national security aims, they also have a strong commercial interest in maintaining access to lucrative overseas markets. Companies often rely on American government advocacy to push back against CCP and other restrictive regimes and ensure global market access and competitiveness.

---

[32] "IQT Quarterly Recap — Summer 2024," accessed May 12, 2025, https://www.iqt.org/library/iqt-quarterly-recap-—-summer-2024.
[33] "Cybersecurity Maturity Model Certification (CMMC)," DoD CIO, accessed April 19, 2025, https://dodcio.defense.gov/cmmc/About.
[34] Kathryn Moretti, "Incentivizing Small Businesses to Grow to and Through the 'Tween Phase," April 5, 2025, 12.
[35] James Tager, "Made in Hollywood, Censored by Beijing," PEN America, August 5, 2020, https://pen.org/report/made-in-hollywood-censored-by-beijing/.

In recent years, the relationship between leading American social media platforms and the federal government has been stressed, with accusations of government heavy-handedness regarding content moderation and access to platform data. Nevertheless, companies have shown a willingness to engage on issues like promoting digital literacy, labeling state-sponsored content, and allowing community review of online content. Corporations like Meta, Google, and Amazon face increased pressure to act in the face of antitrust litigation and new regulatory frameworks like the European Union Data Services Act and the General Data Protection Regulation (GDPR).[36] Ultimately, American Big Tech wants secure global revenue streams, protection from liability, and predictable regulatory environments. The evolving relationship between the government and these platforms is one of mutual dependency but also strategic friction, with neither side fully aligned on the balance between innovation, accountability, and democratic values.

Private Citizens' Interests

Private citizens' stake in cybersecurity concerns the protection of their data, access to secure services, and economic opportunities. Their interests span personal security, trust in public systems, and the societal benefits of resilient infrastructure. Citizens benefit from secure technologies developed through public-private partnerships, educational initiatives like NICE, and legislative programs like the CHIPS Act, which provide pathways into high-skill cyber careers and help democratize access to digital literacy.

Private citizen mobilization includes increased public awareness of cyber threats, disinformation, and digital responsibilities. Efforts like media literacy campaigns, cyber hygiene education, and

[36] "The EU's Digital Services Act," October 27, 2022, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

labeling of state-sponsored content help build societal resilience. Citizens also play a crucial role in surge capacity planning, potentially serving in volunteer cyber auxiliaries or reserve structures during emergencies, akin to National Guard models.[37] Doing so will expand the nation's rapid response capability and integrate civic-minded technical talent into defense efforts.

Trust is a cornerstone of citizen engagement. Transparent government policies, ethical technology use, and secure digital infrastructure reinforce public confidence. Citizens expect accountability in the deployment of AI and surveillance technologies, and they value privacy protections and consumer rights.

Operational Framework and Analysis

To secure America's strategic advantage in the digital domain, this section applies an operational framework that links high-level challenges to actionable lines of effort across four key areas: innovation, digital supply chain resilience, workforce development, and informational superiority. Each LOE is structured to identify key issues, propose recommended tasks, and assess the broader implications for national defense, economic competitiveness, and democratic stability. This structured analysis offers a roadmap for institutional reform and public-private collaboration, enabling the United States to outpace adversaries and build enduring digital resilience.

Each recommended task within the LOEs is further organized into one of four task categories, which reflect the functional character of the effort required. *Institutional Reform* addresses structural modernization, governance, and policy adjustments needed across defense and federal agencies. *Private Sector* captures efforts that strengthen collaboration and capacity-building

[37] Joel Smith, "National Public-Private Cybersecurity Strategic Initiative," March 23, 2025.

between government and industry. *Cyber Architecture* includes tasks that establish frameworks, technical standards, and cybersecurity operational models. Finally, *Education & Influence* encompasses tasks focused on public awareness, information literacy, and cultural resilience in the information environment.

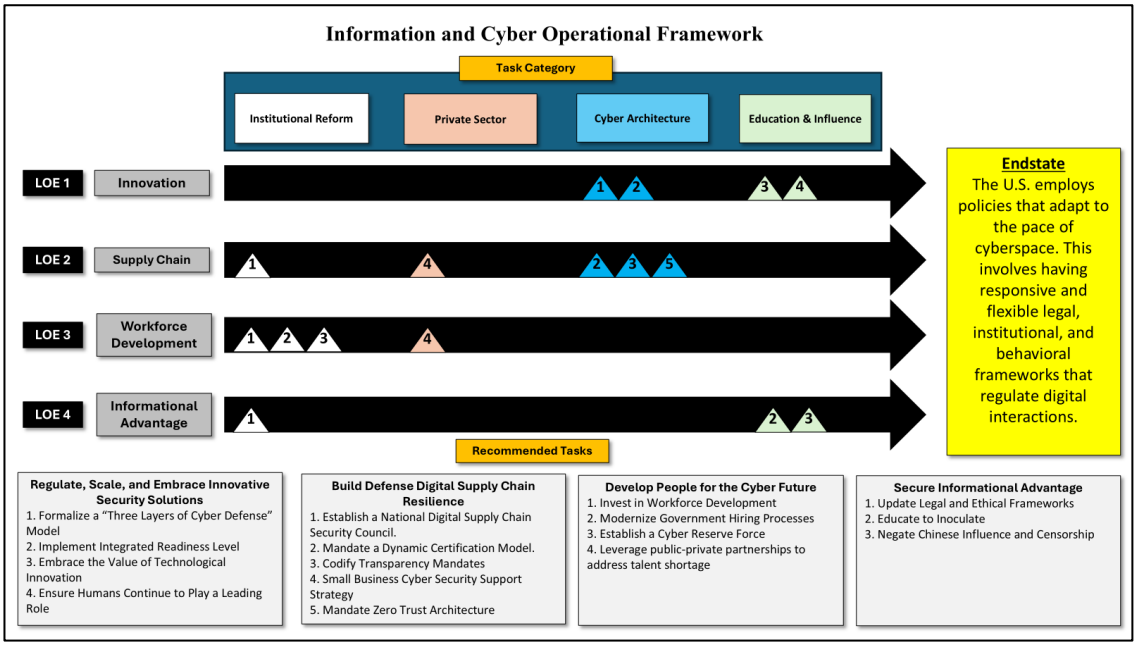

Figure 1: Information and Cyber Operational Framework

LOE 1 - Regulate, Scale, and Embrace Innovative Security Solutions

Since the Morris Worm, the United States has ceded many technological advantages due to weak cybersecurity controls. In the development of its cyber infrastructure, the U.S. prioritized speed and productivity over security, leading to economic gains but accumulating security risks. Weak controls led to billions of dollars of IP theft and exposed material security weaknesses within the DoD and the DIB. The private sector's innovative solutions are a key input to mitigating these weaknesses. However, harnessing these solutions requires the government to implement effective regulation, focus exclusively on scalable security solutions across the entire force, and

ultimately embrace innovation as the driver of the United States' technological advantage over the coming decades.

Key Issues and Challenges

Ineffective Regulation. Although innovative security solutions provide exquisite cyber capabilities, they also introduce material risks. To prevent exploitation, ensure accountability, and protect sensitive data, the DoD's governance, risk, and compliance (GRC) responsibilities must mature faster through automated and effective regulation that balances innovation and security.

The DoD's current regulation framework is slow and ineffective due to a reliance on manual processes and the dependence on the DIB to self-regulate. Following guidance from the DoD Chief Information Officer, the Defense Contracting and Management Agency (DCMA) assesses the DIB's compliance with the Cybersecurity Maturity Model Certification (CMMC).[38] MMC's three-tiered regulatory framework ensures DIB implementation of security controls to protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). [39] A combination of the Defense Counterintelligence and Security Agency (DCSA), the National Security Agency (NSA), and their lower-echelon counterparts work to implement security controls for classified information in the DIB.[40] While the CMMC provides the framework to safeguard national security capabilities in the DIB, DCMA is not resourced or equipped with the

[38] U.S. Department of Defense, "*DoD Directive 5144.02: DoD Chief Information Officer (DoD CIO)*," November 21, 2014, incorporating Change 1, September 19, 2017, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/514402p.pdf, accessed May 1 12, 2025.
[39] Defense Contract Management Agency, "DIBCAC," accessed May 9, 2025, https://www.dcma.mil/DIBCAC.
[40] Defense Counterintelligence and Security Agency, "NISP Cybersecurity Office (NCSO)," https://www.dcsa.mil/Industrial-Security/NISP-Cybersecurity-Office-NCSO/, accessed May 12 2025; National Security Agency, "Cybersecurity," https://www.nsa.gov/Cybersecurity/, accessed May 12 2025.

expertise to fulfill its regulatory responsibilities. As a result, it relies on third-party contractors to certify companies' compliance with the CMMC.

Even though the CMMC requires the DIB to implement controls for established security practices, the regulatory environment for emerging technologies remains immature. Laws and DoD policies have not kept pace with the ethical and legal questions posed by autonomous systems. For example, the application of AI raises concerns about accountability, bias, and transparency, which underscores the need for policy and guidelines to drive the regulation of emerging technologies. Without regulatory guidance, the DoD cannot ensure the responsible development and deployment of advanced capabilities. Furthermore, the lack of regulations for comprehensive testing of AI risks increases vulnerabilities and unintended consequences, which can compromise mission effectiveness.

Regulation includes compliance with established cyber practices and emerging technologies and acquiring and sustaining security solutions. Unfortunately, the acquisition process is slower than the operational tempo of cyber threats. Traditional approaches emphasize long-term planning and fixed deliverables, which are ill-suited to the iterative nature of software development. As a result, the delivery of cybersecurity capabilities arrives too late to address current vulnerabilities or lacks the flexibility to evolve with the threat landscape.

Segmented, Legacy Security Solutions Restrict Scalability. The DoD's bureaucracy, risk aversion, and limited funding have created a cybersecurity environment that is either segmented, antiquated, or both. These are significant challenges that limit scalability. DoD's legacy systems are typically implemented for a specific client rather than the entire force. Due to their singular focus, interoperability and seamless integration were not prioritized, resulting in segmented and siloed solutions. For example, the DoD developed the Global Information Grid (GIG) to "enable

the access to, exchange, and use of information and services throughout the Department and with non-DoD mission partners."[41] Although the vision of the GIG was to facilitate sharing across DoD agencies and services, the implementation faced interoperability issues because of legacy systems and custom-built tools.[42]

The Pentagon recognizes the importance of integrated systems and has even developed an "integrated readiness level" that describes the " maturity level of integrating one system into another." [43] This, however, has never been fully implemented, leaving the integration and scalability challenge unresolved.

Even if the DoD wanted to transition to security solutions that could scale across the force, regulatory and compliance barriers prevent it. For example, the authority to operate (ATO) requirement for cutting-edge security solutions would dramatically slow the deployment of a state-of-the-art, AI-enabled threat detection solution into production. In the meantime, America's adversaries can exploit the vulnerability. While ATO requirements are understandable, the delays incurred by ATO requirements may become crippling.

Fear of Technology. To fully benefit from technological innovations, the Department of Defense and the defense industrial base must embrace technology and commit to using it to its full capability. Unfortunately, this is often hindered by an aversion to change and risk. Many policymakers are comfortable with traditional approaches and hesitant to learn new strategies. They may also worry about the negative impacts of innovation (e.g., cybersecurity vulnerabilities

---

[41] Department of Defense, Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise, Version 1.0 (June 2007), prepared by the DoD CIO.

[42] U.S. Government Accountability Office, "DOD's Global Information Grid: Background and Issues for Congress," GAO-04-858 (July 2004), https://www.gao.gov/assets/gao-04-858.pdf.

[43] Clarence Eder, Thomas A Mazzuchi, and Shahram Sarkani, "Beyond Integration Readiness Level," July 2017, https://www.dau.edu/sites/default/files/Migrate/ARJFiles/ARJ82/ARJ82_Article%205%20-%2016-766%20Eder.pdf.

caused by new technology or innovation's impact on their job security). Failure to overcome these aversions will cede the innovation advantage to our adversaries and diminish our national power. Successfully embracing technology, however, poses another challenge: the possibility of degrading human expertise and judgment. As the private sector begins to use AI to perform cybersecurity tasks, human operators risk becoming passive monitors rather than active participants in security operations. This can erode the operators' capacity for critical thinking, particularly in complex or ambiguous situations where human insight is indispensable.

Recommended Tasks:

The following recommendations address the three main challenges underlying policy and innovation identified throughout this LOE.

Formalize a "Three Layers of Cyber Defense" Model: The financial services industry successfully employs a three lines of defense approach to cyber risk management. The DoD should adopt this model for its cyber risk management and compliance practices. Operational units that execute cyber defense or DIB companies that build security tools serve as the first layer of defense. The second layer would consist of major command functions that provide oversight, guidance, and monitoring of the first line. The third layer is service or agency-wide functions that conduct assessments and audits to ensure alignment with cyber standards and regulations.

The three layers of the cyber defense model ensure innovation is well-managed with the proper guardrails. This framework will allow the DoD to conduct proactive risk identification and effective mitigation while enforcing compliance with laws and regulations. It enables innovation by facilitating timely responses to emerging threats while balancing the effective implementation of risk management from the financial services industry. The DoD will improve its ability to

prevent cyber breaches, protect customer data, and maintain business operations. This recommendation standardizes and streamlines defense cybersecurity oversight responsibilities under the leadership of the DoD CIO and fosters defense-industrial teaming between agencies and classification levels.

Implement Integrated Readiness Levels. The DoD must implement Integration Readiness Levels (IRLs) as a framework across all services and agencies to evaluate and ensure the interoperability of innovative security solutions. Adopting IRLs with Technology Readiness Levels (TRLs) allows a standard framework to assess the integration maturity between DoD applications and platforms. More importantly, it underscores the need to prioritize interoperability through seamless integration early in development.

Implementing IRLs increases the transparency for the potential scalability of security solutions and reduces the risk of deploying complex systems. It allows the DoD to make targeted investments for mature solutions to integrate into the larger architecture. While detractors of IRLs argue that they slow the development of innovative products by adding overhead, in the long term, they accelerate the deployment of tools at scale by streamlining the acquisition process. Ultimately, IRLs reduce the cyber risk of a security solution by decreasing the number of segmented tools and increasing system resilience.

Embrace the Value of Technological Innovation. Senior leaders in the DoD and the DIB must lead a mindset change regarding technology. Leadership must promote and reward experimentation, adaptation, and cross-functional collaboration to enable effective technological adoption. Leaders should also ensure that examination and evaluation of the latest innovative technologies are embedded into strategic planning cycles and elevate individuals with technological expertise into roles where they can evangelize the effective use of technology. The

DoD and DIB must commit to effectively training impacted employees on the benefits and uses of new technologies and adjust procedures and processes to ensure the technologies' successful adoption. Finally, the DoD should demand that managers evaluate their employees' ability to promote and leverage new technology to advance national interests.

One way to overcome institutional hesitancy towards technology is to highlight innovation successes regularly to the workforce. For example, to overcome anxiety about AI, the DoD should explain its value in improving cybersecurity by enhancing threat detection and response time. The DoD should also emphasize how AI can automate repetitive yet critical tasks (like vulnerability scanning) to develop secure code less prone to human error.

Ensure Humans Continue to Play a Leading Role. As technological advances take on more and more human functions, leaders and managers must keep their workforce actively engaged in working with and monitoring technology and provide the workforce the authority and ability to intervene when circumstances warrant. As a leading AI expert stated, "Humans will not lose to machines; they will lose to humans with machines."[44] Leaders and managers need to adopt this as a mantra. The DoD and DIB cannot ignore the benefits of technology. Instead, they must partner with technology to achieve success.

Special emphasis must be placed on increasing the cybersecurity hygiene of small and medium-sized defense contractors by offering technical assistance, cost-sharing programs, and access to threat intelligence to reduce barriers to compliance.

Synthesis

Ensuring cybersecurity superiority in the 21st century demands more than incremental adaptation; it requires a comprehensive transformation across strategy, systems, and culture. As

[44] Industry Study Class, March 27, 2025.

cyber threats grow in sophistication and strategic competitors exploit technological asymmetries, the United States must close the innovation gap and build a resilient digital foundation that supports national defense, economic competitiveness, and democratic values. The above recommendations offer a roadmap for aligning innovation with mission outcomes, operational agility, and long-term resilience.

Implementing these actions will require sustained leadership commitment, resource investment, and a collaborative mindset across public, private, and international partners. Agencies must institutionalize continuous innovation as a strategic function, not an occasional initiative, and hold leaders accountable for progress in integrating emerging technologies securely. By embracing technology as a core determinant of national power and acting with urgency and purpose, the United States can shape the future of cyberspace to its advantage and ensure freedom of maneuver in an increasingly contested domain.

LOE 2 - Build Defense Digital Supply Chain Resilience

The convergence of pandemic-induced disruptions, geo-political instability, and intensifying great power competition has exposed weaknesses in the United States' defense logistics architecture. Although historically resilient, the DIB now operates within a complex, digitized environment where the opacity of supply chains and reliance on fragmented global networks undermine national security objectives. Events like the COVID-19 pandemic and the war in Ukraine disrupted access to critical components. At the same time, China's deliberate strategic posture, centralizing its logistics ecosystem under state control, has illustrated the competitive disadvantage of America's decentralized model. As adversaries like China pursue tightly coordinated, government-backed digital logistics strategies, the United States faces mounting

pressure to modernize its infrastructure or risk strategic disadvantage.[45] [46] These challenges underscore a fundamental truth: the traditional logistics paradigm is no longer sufficient to sustain military readiness in a contested global order.

Key Issues and Challenges

Vulnerability and Lack of Cohesion. The distributed and fragmented nature of the DIB complicates efforts to build a coherent and resilient digital supply chain. While standardization initiatives such as the National Institute of Standards and Technology (NIST) and CMMC frameworks provide baseline expectations, implementation varies widely.[47] The absence of a central governance body exacerbates these disparities. As digital integration proceeds unevenly, adversaries may exploit inconsistencies between well-protected and under-secured nodes within the supply chain. This fragmentation introduces cascading risks where localized disruptions can spread quickly across critical systems. Moreover, disconnected digital architectures hinder rapid adaptation and centralized situational awareness, two factors essential for resilience in contested environments.

> *The clearest definition of Information Communications Technology Supply Chain Risk Management ICT-SCRM risk is under the Committee on National Security Systems. (CNSS) directive (CNSSD) 505 [9]: "The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system" (The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806).*

[45] "The Geopolitics of Rare Earth Elements 2019," n.d.
[46] Gustavo Ferreira and Jamie Critelli, "China's Global Monopoly on Rare-Earth Elements," *The U.S. Army War College Quarterly: Parameters* 52, no. 1 (March 9, 2022): 57–72, https://doi.org/10.55540/0031-1723.3129; Izabela Rojek et al., "Review of the 6G-Based Supply Chain Management within Industry 4.0/5.0 Paradigm," *Electronics* 13, no. 13 (July 4, 2024): 2624, https://doi.org/10.3390/electronics13132624.
[47] NIST. Special Publication 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Gaithersburg, MD: NIST, May 2022.

Cybersecurity Risks. While the United States must fully leverage digital logistics systems, this embrace widens the attack surface for cyber threats. Global suppliers, some of whom operate within or are influenced by adversarial regimes, increasingly provide components like AI algorithms, Internet of Things (IoT) sensors, and blockchain networks. [48] Hardware and software dependencies on Chinese manufacturing create embedded vulnerabilities and backdoor access risks. Internally, many small DIB entities remain under-resourced, lack dedicated cyber personnel, and operate without automated threat detection or segmentation protocols. The over-reliance on periodic compliance audits fails to match the tempo of modern cyber threats, which exploit real-time vulnerabilities that static controls cannot detect. Additionally, reliance on AI for logistics decisions without appropriate human oversight can amplify risks if adversaries compromise inputs or models.

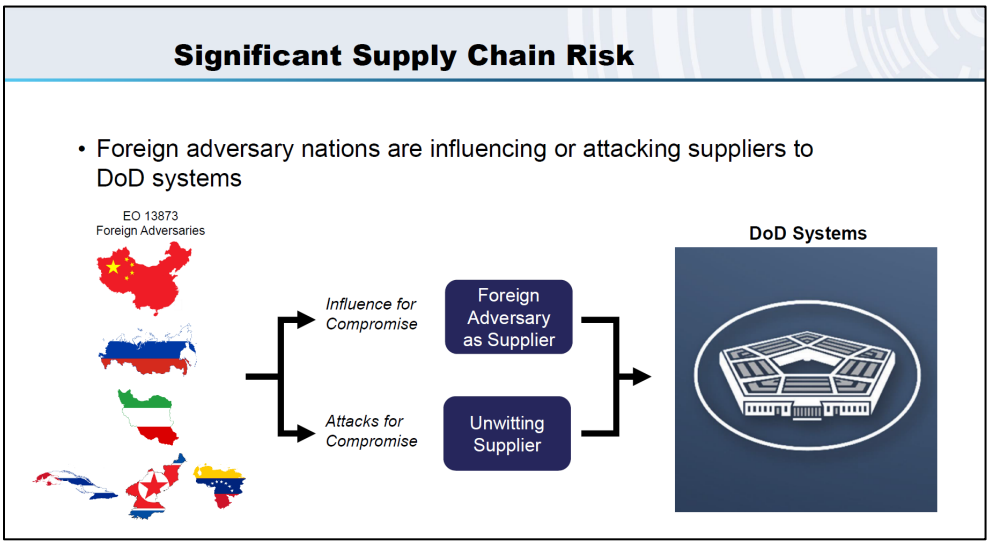

Figure 2: Foreign adversary nations' influence and impact on suppliers to DoD systems[49]

[48] Mohammad I. Merhi and Antoine Harfouche, "Enablers of Artificial Intelligence Adoption and Implementation in Production Systems," *International Journal of Production Research* 62, no. 15 (August 2, 2024): 5457–71, https://doi.org/10.1080/00207543.2023.2167014.
[49] Mr. Paul De Naray, Principal Engineer at Aerospace Corporation. Brief to Eisenhower School Global Supply Chain and Logistics Concentration Elective

Interoperability. Digital modernization within the defense sector often progresses through isolated efforts, resulting in an assortment of systems with limited interoperability. Differing standards and data protocols among agencies and contractors affect integration and coordination. This problem is technical and organizational, reflecting a lack of unified architecture and common data models. Overcoming this challenge requires both investment and cultural transformation. The opportunity cost of maintaining disjointed systems includes delayed decision-making, redundant processes, and diminished capacity for predictive analytics across supply chains.

Acquisition and Implementation Barriers. Despite the availability of proven digital tools, outdated procurement models hinder timely adoption. The federal acquisition process often emphasizes risk aversion over innovation, prioritizing compliance and cost control at the expense of adaptability. Stove-piped acquisition practices within agencies further limit joint experimentation or shared infrastructure investment. Program offices may lack the technical literacy and operational urgency to prioritize digital supply chain capabilities. These constraints delay the integration of cutting-edge tools and contribute to uneven progress across mission-critical programs.

Data Quality and Governance. The effectiveness of digital logistics systems is inextricably linked to the quality, availability, and governance of data. Many legacy systems within the defense enterprise operate in siloed environments with inconsistent data collection, limited tagging, and minimal interoperability. As a result, digital tools are fed incomplete or outdated data, undermining the fidelity of decision-making. Poor metadata practices and the absence of shared taxonomies compound this problem. Additionally, there are inadequate governance frameworks to ensure accountability over data stewardship, particularly in multivendor

environments. Without trusted, real-time data flows, the promise of digital logistics remains unfulfilled.

Information Sharing and Trust. While several public-private initiatives exist, such as the Information and Communications Technology (ICT) Supply Chain Risk Management Task Force, there remains a lack of institutionalized trust and clearly defined protocols for information exchange.[50] Companies may hesitate to share threat intelligence or vulnerability disclosures with government entities out of concern for regulatory penalties, reputational harm, or competitive disadvantage. Conversely, government actors often fail to reciprocate with timely, actionable insights. Legal ambiguity around data use, ownership, and liability further stymies collaboration. Building resilient digital logistics requires not only technological integration but also the establishment of a trusted operational community with shared incentives and protections.

Recommended Tasks

Establish a National Digital Supply Chain Security Council. This organization will have statutory authority and will comprise leadership from the DoD, DHS, the General Services Administration (GSA), and the industry. The council will harmonize policy, resolve interagency conflicts, and serve as the operational hub for coordinating digital logistics modernization. This body will reduce fragmentation by enforcing a unified governance framework across federal and defense supply chains.

Mandate a Dynamic Certification Model. Continuous monitoring must replace static compliance models. Automated telemetry, real-time analytics, and behavior-based alerting systems would form the foundation of a new trust architecture. Contractors would submit telemetry to secured

[50] "GAO Report. Information and Communications Technology, 2023" n.d.

government nodes or trusted third parties, enabling real-time risk scoring and proactive mitigation. Such a model closes the temporal gap between audit and attack.

Codify Transparency Mandates. Suppliers must submit Software and Hardware Bills of Materials (SBOMs and HBOMs) with documented lineage for software code and hardware components. This measure enables upstream threat identification and provides critical context for vulnerability triage. Private sector actors like Oracle already possess mature SBOM capabilities that could serve as implementation models.

Small Business Cyber Security Support Strategy. Many innovation-driven SMBs within the DIB cannot afford high compliance costs. The government shall offer cybersecurity grants, tax incentives, and access to subsidized compliance tools. Enabling participation from these actors will preserve innovation density while raising the security baseline.

Mandate Zero Trust Architecture. This means enforcing granular access controls for users, devices, and APIs. Security must be embedded throughout the Development, Security, and Operations lifecycle, from code scanning and dependency checks to release signing and runtime monitoring. [51] Blockchain should also be employed for component traceability, using smart contracts to restrict access to verified artifacts. Centralized Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA) platforms will integrate log data across suppliers, enabling anomaly detection at the system level. Lastly, the supply chain infrastructure must be segmented with redundant pathways to contain breaches and ensure continuity.

---

[51] Department of Defense. *Zero Trust Reference Architecture v1.0.* Washington, D.C.: DoD Chief Information Officer, July 2022.

Synthesis

Modernizing defense logistics through digital platforms is not simply a matter of efficiency but a national security imperative. The ability to move, track, and safeguard critical materials across global supply chains directly affects military readiness, deterrence, and warfighting capability. Equally important is the ability to discern provenance, both material and digital. As strategic competitors like China build centralized, state-backed logistics systems with global reach, the United States cannot afford to rely on outdated, fragmented, and reactive models.

To close the gap, the United States must develop a national digital logistics strategy that aligns the government and industry with common goals. It must also raise the cybersecurity baseline across the defense supply chain, including small businesses operating below the cyber poverty line. It must establish clear benchmarks for success, ensuring digital logistics modernization becomes a permanent capability rather than a passing initiative.

LOE 3 - Develop People for the Cyber Future

The United States' workforce has not kept up with the pace of cyber innovation. The American government urgently needs to overhaul its current strategy and allocate greater resources to build a workforce capable of competing in cyberspace. Training individuals is only one part of the solution, however. Technology, such as AI, must be leveraged to increase productivity and maximize every person.

Key Issues and Challenges

Lack of Qualified Cybersecurity Personnel. The United States faces a shortage of qualified personnel to fill cybersecurity positions. In 2024, there were over 1.25 million cybersecurity workers in the United States. However, they only fill 83% of available positions, leaving almost

half a million job openings.[52] Information Security Analyst jobs are projected to grow 33% between 2023 and 2033, worsening the situation.[53] In 2022, only about 7,000 students received bachelor's degrees in Computer Information Systems Security, Auditing, or Information Assurance, and 110,000 students graduated from U.S. colleges with bachelor's degrees in "related" fields.[54]

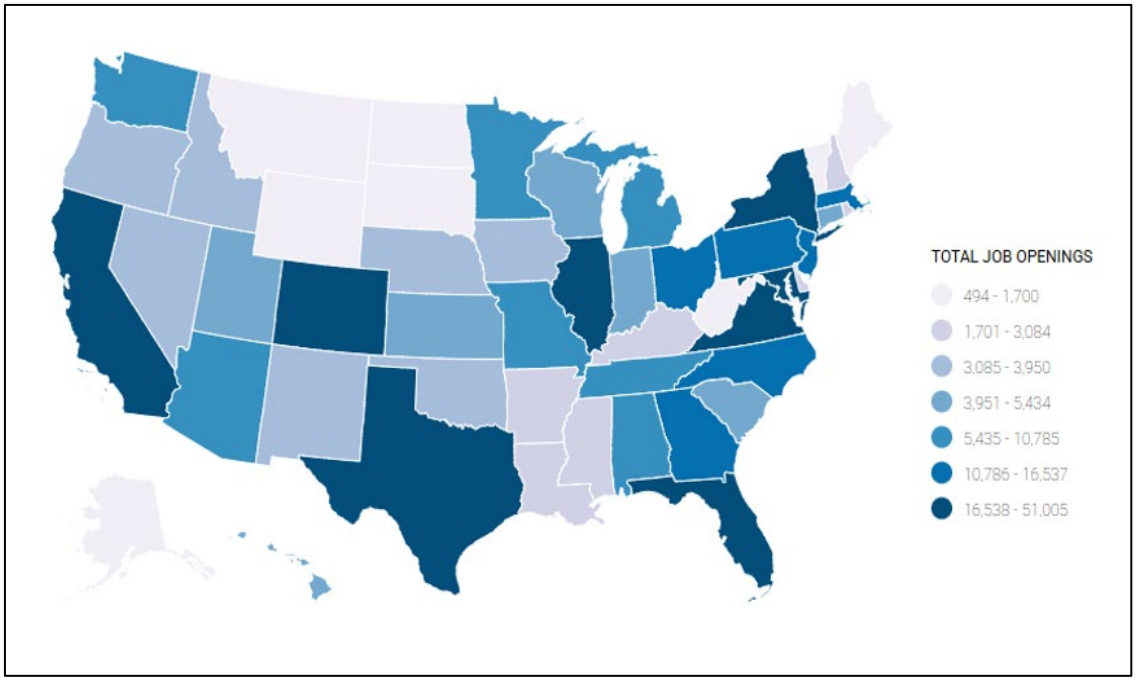

Figure 3: Cybersecurity Supply/Demand Heat Map by Cyber Seek[55]

Much of the training conducted in American universities does not translate to the workforce. In 2022, non-citizens on temporary visas earned 41% of cybersecurity Master's and 61% of

[52] "Cybersecurity Supply And Demand Heat Map." Accessed April 18, 2025. https://www.cyberseek.org/heatmap.html.
[53] Bureau of Labor Statistics. "Information Security Analysts." Accessed March 19, 2025. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[54] Hogan, M, K Lilienthal, A Bean de Hernandez, P McHugh, CA Arbeit, and P Sullivan. "Cybersecurity Workforce Data Initiative." National Center for Science and Engineering Statistics (NCSES), May 2024. https://ncses.nsf.gov/initiatives/cybersecurity-workforce-data-initiative.
[55] "Cybersecurity Supply And Demand Heat Map," accessed May 12, 2025, https://www.cyberseek.org/heatmap.html.

Doctorate degrees from American Universities.[56] International students face challenges remaining in the United States after graduation, especially when prospective jobs require security clearances.[57] These legal and bureaucratic barriers lead to a paradox in which the United States trains highly skilled individuals but does not retain them in positions that contribute to national defense or critical infrastructure protection.

Outdated Hiring Policies. The National Cyber Workforce and Education Strategy (NCWES) of 2023 emphasizes the need to streamline hiring processes and use skills-based hiring to bring in critical cybersecurity workers.[58] Hiring practices across federal agencies are frequently outdated, overly bureaucratic, and poorly aligned with modern workforce expectations, taking months from application to onboarding. Education requirements like four-year degrees are obsolete and can exclude otherwise capable candidates. Security clearance vetting for government jobs causes delays, causing applicants to find employment elsewhere. The NCWES's success depends on agencies' willingness to abandon legacy systems and embrace structural reform at every stage of the hiring process. It is still unproven due to its recent implementation.

Talent Retention. Retention of skilled employees in government positions remains a challenge. Government cyber professionals leave after acquiring foundational experience and certifications, lured by private sector roles that offer higher compensation, faster career advancement, and more flexible working conditions. Public sector positions often provide fewer incentives for professional growth, rely on rigid pay scales, and use outdated performance management systems. These issues collectively weaken morale and increase attrition.

---

[56] Hogan, 2024.
[57] Hogan, 2024.
[58] "National Cyber Workforce and Education Strategy-Unleashing America's Cyber Talent." Office of the National Cyber Director, Executive Office of the President, the White House, July 31, 2023. https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

A technical talent shortage affects defense supply chains by reducing production speed, increasing costs, and elevating the risk of insecure code. In critical infrastructure sectors, engineer shortages translate into delayed patching, deferred modernization, and the accumulation of technical debt, which increases the likelihood of successful cyber intrusions. In this way, labor shortages ripple outward and affect the security and performance of entire sectors.

Education Initiatives. Efforts are underway to begin developing the cyber workforce well before college. Programs like NSA's Teach Cyber and GenCyber bring middle and high school students into contact with cyber principles through experiential learning.[59] The Elementary School Cyber Education Initiative (ESCEI) promotes cyber awareness and responsible digital behavior among younger students.[60] Junior Reserve Officer Training Corps (JROTC) programs have a dedicated cyber program, offering competitions like CyberPatriot to teach practical skills in a team-based environment.[61, 62] These programs bridge the gap between everyday digital exposure and professional pathways, offering early intervention that counters the perception of cybersecurity as overly technical or inaccessible.

At the postsecondary level, programs such as the CyberCorps Scholarship for Service provide tuition support to university students in exchange for a commitment to public service, like the Reserve Officer Training Corps (ROTC) does for the military.[63] Yet these programs remain

[59] "Teach Cyber Impact Report 2019-2024." DARK Enterprises, Inc. Accessed April 18, 2025. https://teachcyber.org/wp-content/uploads/2024/12/DARKEnterprises-ImpactReport-Dec2024.pdf.
[60] "ELEMENTARY SCHOOL CYBER EDUCATION INITIATIVE." Accessed April 18, 2025. https://www.uscyberpatriot.org/Pages/Special%20Initiatives/Elementary-School-Initiative.aspx.
[61] "Cyber Program Overview – U.S. Army JROTC." Accessed April 18, 2025. https://www.usarmyjrotc.com/cyber/.
[62] "What Is CyberPatriot?" Accessed April 18, 2025. https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx.
[63] Mo, Seeyew. "Service for America: Cyber Talent Is Everywhere and Opportunity Should Be Too | ONCD." The White House, October 18, 2024. https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/10/18/service-for-america-cyber-talent-is-everywhere-and-opportunity-should-be-too/.

limited in scale and scope, and they often struggle to compete with private employers who can offer better pay and faster hiring timelines.

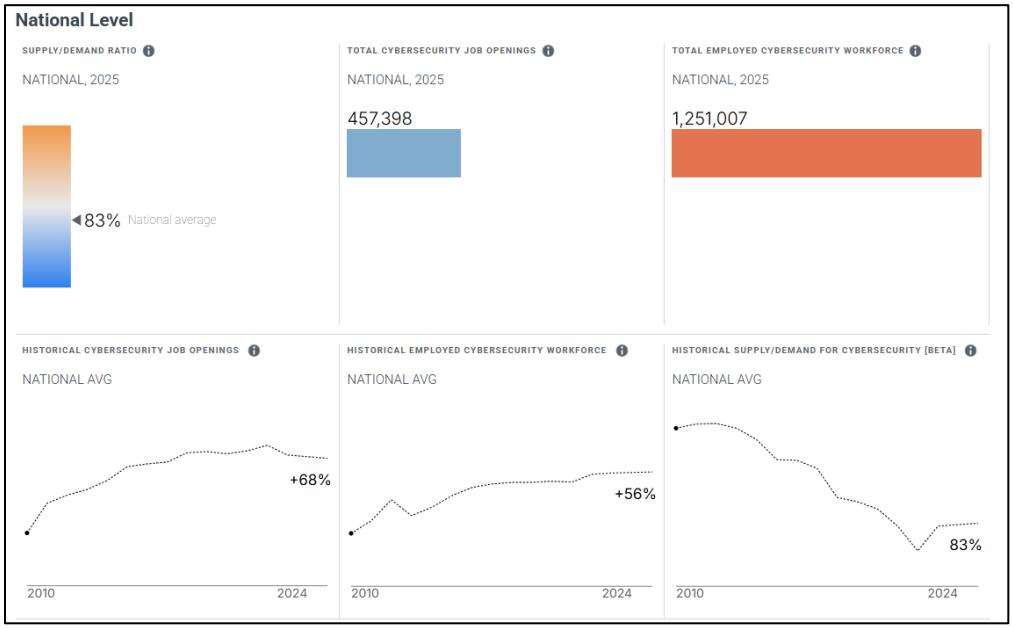

Figure 4: National Level Cybersecurity Supply/Demand Chart by Cyber Seek [64]

Recommended Tasks

To prepare American citizens to operate in an increasingly digital world, the United States should pursue four core strategies: invest in workforce development, modernize government hiring and retention systems, establish a Cyber Reserve Force, and leverage public-private partnerships (PPP).

Invest in Workforce Development. Investment in workforce development is critical to broadening the talent pipelines. Federal funding should support cybersecurity education from elementary school through postgraduate training to build cyber literacy from an early age. Educational institutions must offer flexible pathways, including certificate programs, boot camps, and

[64] Ibid

competency-based credentials. Academia should encourage employer involvement in curriculum design by funding internships, apprenticeships, and mentorship programs. The government must actively collaborate with industry and academia to develop joint training programs and talent exchanges. These collaborations would give government employees access to cutting-edge tools and provide private sector workers with experience directly related to government challenges. Leaders at all levels must receive cyber risk awareness training to understand the strategic importance of cybersecurity.

Modernize Government Hiring Processes. Current government procedures are too slow and inflexible to keep up with the pace of cyber threats. Policymakers should remove unnecessary degree requirements, expand the use of skills-based hiring, and streamline security clearance processes. These reforms would allow agencies to access a wider talent pool and onboard new hires faster. Competitive compensation packages, support for flexible work arrangements, and clear career development pathways must accompany streamlined hiring. Performance management systems should reward innovation, collaboration, and continued learning. Modernized human resources systems will improve hiring outcomes and increase retention and employee satisfaction.

Establish a Cyber Reserve Force. Modeled on military reserve components, this force would consist of trained professionals from the private sector who would mobilize to support national cyber operations during periods of heightened risk or crisis. Regular training sessions maintain readiness, ensure access to credentials, and facilitate knowledge sharing. This model would enhance capacity during emergencies and foster cross-sector trust and resilience.

Leverage public-private partnerships to address talent shortages. Collaborative training programs, cyber fellowships, and knowledge exchange initiatives can help align government and

industry practices, foster trust, and reduce duplication of effort. By establishing common frameworks for skills assessment and performance, such partnerships can increase workforce mobility and support broader ecosystem resilience. When properly structured, these collaborations benefit all participants while enhancing national preparedness.

Synthesis

The speed of cyber is outpacing the people who work with it. Consumers, employees, and technical experts who depend on the digital environment must understand and trust that it is secure. Without a cyber-literate population and cooperation between government, industry, and academia, the institutions that make up daily life in America are at risk. The government needs to be able to hire and retain top talent, encourage the development of cybersecurity career paths and educational opportunities, and remain competitive with private industry, allies, and adversaries.

LOE 4 - Secure Informational Advantage

Information is a vital instrument of national power. Disinformation, data privacy concerns, and autocratic censorship have eroded public trust, fed political and social polarization, and allowed America's adversaries' global narratives to flourish. Maintaining an advantage in the digital domain requires a healthy media ecosystem in which informed and engaged citizens are inoculated against censorship and false narratives. The United States must use its democratic advantage to shape the future of the information domain.

Key Issues and Challenges

The Impact of Digital Communications on Disinformation. The era of instantaneous, digital communications has democratized speech but has also unleashed a pandemic of disinformation

and divisiveness. Adversarial states and malign actors take advantage of cyberspace to conduct sophisticated online campaigns to undermine democratic institutions.[65]

Regulatory Gaps in the Modern Information Ecosystem. Unfortunately, the internet, the backbone of the modern information environment, has outpaced traditional regulatory frameworks for media content, licensing, and liability. This has created significant accountability gaps. Online platforms often portray themselves as intermediaries rather than traditional publishers, complicating efforts to apply regulatory standards. Social networks lack transparency regarding where online content originates and mask connections to state actors.

Furthermore, current law allows social media companies and online advertisers to profit from user data without meaningful consent. In turn, malign actors and platforms manipulate citizens' beliefs, decisions, and behavior through sensationalized and harmful content. Corporations face few penalties for data breaches or misuse, externalizing the risks onto the individuals they profit from.

The Spread of Disinformation as a Public Health Crisis. The mass spread of disinformation represents a pandemic that threatens the Western international order: just as a pathogen spreads through a population, false and dangerous information proliferates rapidly through social networks and media.[66] Policymakers worldwide are increasingly adopting a public health approach focusing on awareness, contact tracing, exposure, resilience, and treatment to contain this global malady. Various studies have demonstrated that by exposing individuals to weakened forms of misinformation- and disinformation, experts can *inoculate* them against more malicious

[65] Daniel Fried and Alina Polyakova, *Democratic Defense against Disinformation* (Washington, DC: Atlantic Council, 2018).

[66] Nicholas Rabb et al., "Cognitive Cascades: How to Model (and Potentially Counter) the Spread of Fake News," *PLOS ONE* 17, no. 1 (January 7, 2022): e0261811, https://doi.org/10.1371/journal.pone.0261811; Scott C Fenton, "Misinformation Contagion: A View Through an Epidemiological Lens" (Monterey, CA, Naval Postgraduate School, 2019), Calhoun DSpace Repository.

information campaigns. Herd immunity can be attained when a sufficient portion of the population is trained to resist false narratives.[67]

China's Global Censorship and Media Control. China exerts censorship and coercion both at home and abroad to silence speech and stem the flow of pro-Western content. The Chinese Communist Party (CCP) has long censored media content within China but, in recent decades, has made concerted efforts to suppress undesirable narratives abroad.[68] This includes active global expansion of Chinese news agencies, the expulsion of Western outlets, surveillance and immigration pressure on foreign correspondents, and reported cyber-attacks on American media.[69] As a result, the CCP has restricted international media coverage of serious issues like Uyghur repression, religious persecution, child and forced labor, sterilization campaigns, organ harvesting, and gray-zone conflicts in the South China Sea.

China's Influence on Hollywood and Global Media. China has coerced the American film industry, a major element of the United States' soft power. The CCP banned numerous movies from screening in China, forced MGM Studios to rewrite a *Red Dawn* reboot with North Korean invaders instead of Chinese, and even censored Winnie the Pooh when a meme compared Xi Jinping to the plump bear.[70] Hollywood studios have routinely modified films for release in China to ensure market access and continued access to Chinese financing. Other countries also use censorship but with less market influence than China. Indeed, the threat of CCP censorship

[67] Fenton, "Misinformation Contagion: A View Through an Epidemiological Lens."
[68] "Beijing's Global Megaphone," Freedom House, 3, accessed March 26, 2025, https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone.
[69] "Beijing's Global Megaphone."
[70] Philip P. Pan, "How China Is Rewriting Its Own Script" (New York Times, November 18, 2018), https://www.nytimes.com/interactive/2018/11/18/world/asia/china-movies.html.; Stephen McDonell, "Why China Censors Banned Winnie the Pooh" (British Broadcasting Corporation, July 17, 2017), https://www.bbc.com/news/blogs-china-blog-40627855.

coerces free-world creators to avoid any potentially offending content, creating a *de facto* worldwide degree of Chinese cultural and informational control.[71]

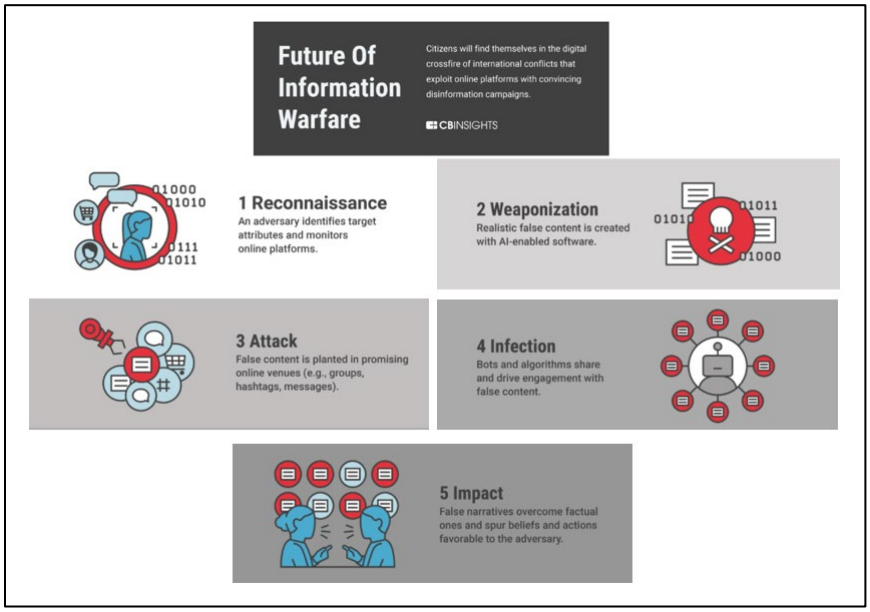

Figure 5: "Disinformation That Kills: The Expanding Battlefield Of Digital Warfare"[72]

Recommended Tasks

The United States requires a whole-of-nation approach to secure the informational domain. The American government should pursue updated legal and ethical frameworks to shape the online ecosystem, nationwide media literacy initiatives to boost societal resilience, and a concerted strategy to combat censorship and project America's story and values across the globe.

Update Legal and Ethical Frameworks. An updated legal and ethical framework based on democratic principles would fundamentally rebalance the digital ecosystem and strengthen individual freedoms and public discourse quality. Rather than censoring content, reforms should target structural abuses, such as undisclosed propaganda, data exploitation, and algorithmic

[71] China's desires now rarely require direct intervention. The last major movie projects critical of the CCP released in 1997 from Disney, Sony, and MGM: *Kundun*, *Seven Years in Tibet*, and *Red Corner* ("List of Films Banned in China," Wikipedia, https://en.wikipedia.org/wiki/List_of_films_banned_in_China, accessed May 13 2025).
[72] "Weaponization of the Future: Digital Warfare & Disinformation | CB Insights," *CB Insights Research* (blog), October 21, 2020, https://www.cbinsights.com/research/future-of-information-warfare/.

manipulation, that undermine the public's ability to engage critically. The federal government should work with social media platforms to publish more details regarding content sources to give consumers greater context. The United States Congress should enact comprehensive privacy legislation granting individuals greater control over their personal data and restricting behavioral tracking and microtargeted manipulation. The government should treat big tech platforms more like traditional publishers to encourage greater editorial responsibility without censorship and to discourage algorithmic amplification of harmful or demonstrably false content.

Educate to Inoculate. The key to achieving inoculation and societal immunity is education. Programs like Finland's national media literacy curriculum, Italy's high school digital literacy program, and Ukraine's IREX "Learn to Discern" initiative represent strategic investments in education that have reduced susceptibility to false narratives.[73] The United States should emulate these best practices and pursue K-12 education reform, including creating nationwide standards for media literacy education and using gamification (i.e., teaching literacy through video/online games) to appeal to young audiences. No barriers exist for states to start implementing media literacy programs now. Private-sector collaboration is also essential. Social media companies and tech platforms must expand initiatives that promote user awareness, such as labeling state-sponsored content and integrating public service announcements (PSAs) directly into user feeds. Education is the most durable, ethical defense against the evolving threat of information warfare.

Traditional approaches to countering disinformation have focused on fact-checking and debunking. However, the American experience during World War II shows that “unskillful

[73] Daniel Fried and Alina Polyakova, *Democratic Defense against Disinformation* (Washington, DC: Atlantic Council, 2018); Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making" (Council of Europe, September 27, 2017).

efforts at ‘rumor-busting’ can cause much harm” and energize the harmful rumors.[74] Rather than directly countering each rumor or rumor-spreader, the government found greater historic success when focused on providing accurate information to fill the vacuum that bad actors exploit. Attempts to correct and suppress disfavored views led many Americans to view previous anti-misinformation programs as censorship.[75] American media institutions and government should instead focus on positive, accurate messaging and equip citizens with the critical thinking skills to recognize the difference between fact and fiction.

Negate Chinese Influence and Censorship. The unfettered flow of culture and ideas is essential to promoting Western values, maintaining global confidence in democracy over autocracy, and defending the informational instrument of power. The United States needs a national strategy that includes legislative and executive action to expose and deter Chinese censorship and that builds partnerships with media and film partners to project America’s story to global audiences. The American government should consider offering credits, from a “Freedom Fund,” to media professionals and studios who find themselves censored in China or other nations, presumably for pro-Western or anti-Communist messages.

Such credits could be proportional to revenues from neighboring free markets such as Japan and South Korea, scaled according to the "lost" market size. In this way, America could reduce China's global media influence without threatening the financial health of the market's dominant Western players. The United States government should source funds from Chinese tariffs to this Freedom Fund, helping to bolster media and voices that are critical of the CCP. Finally, the

[74] Lederle, Cheryl, “What Can Primary Sources Tell Us about Battling Misinformation?” (Library of Congress, February 24, 2022), https://blogs.loc.gov/teachers/2022/02/what-can-primary-sources-tell-us-about-battling-misinformation/, accessed April 30, 2025.
[75] Rubio, Marco, “Protecting and Championing Free Speech at the State Department,” (Department of State, April 16, 2025), https://www.state.gov/protecting-and-championing-free-speech-at-the-state-department/, accessed April 30, 2025.

government should use State Department platforms to help spread pro-democracy, accurate information in contested areas.

Synthesis

Winning in the information domain requires leveraging the influence and innovation of private media and technology platforms and establishing contemporary policy and regulatory frameworks without government censorship. Legal and educational efforts promise to inoculate the American population from malign influence and to set a standard for partners and allies. The United States should transfer the costs of overcoming media censorship to malign state actors via punitive tariffs.

Conclusion

Every company selling a service or product promises that its solution will secure a client's digital infrastructure. While the United States has extraordinary technical ability, a technical or technological solution cannot solve every complex social, political, or human problem. While technical tools are important to countering cyber threats, maintaining the U.S. national security and competitive advantage requires decisive policy reforms. The explosion of attacks in the information and cyber domains suggests that technical solutions have not made the United States more secure. Complicating the problem is that changes to policy and standards are slow because of systemic institutional, bureaucratic, and special interest factors that resist change at the speed of cyber. However, the changing pace of the cyber threat landscape requires decisive policy action.

The reforms in this paper intentionally do not exclusively focus on technology solutions. Instead, this paper recognizes that the nation's policy contains the biggest vulnerabilities to American national security in the information and cyber domain. The efforts to invest in innovative

technologies, build digital supply chain resilience, develop the cyber workforce, and secure the advantage in the information domain present remediations to the nation's biggest material risks. While the LOEs will reduce the risk of cyber-attacks and disinformation from our nation's adversaries, there is no such thing as completely solving the cybersecurity problem. For every policy and technological solution, the threat landscape will adapt its tactics, techniques, and procedures. So long as the United States and its strategic competitors jockey for geo-political leverage, the moves and countermoves in the information and cyber domains will never end. The decisive policy proposed in this paper will patch the United States' bureaucratic vulnerabilities. Still, national security leaders must continue to deliberate and debate the policy governing the information and cyberspace domains. With decisive action, the United States can prevent the next Morris Worm to safeguard national security.

Appendix A - Artificial Intelligence

AI has evolved from an emerging technology to a central force in global competition, economic growth, and national security. Advances in machine learning, natural language processing, and computer vision are reshaping cybersecurity by enhancing both defense and adversary capabilities.

Impact and Use

Companies like Google DeepMind, OpenAI, Microsoft, Amazon, and Google are leading AI research and integration into cloud services, improving efficiency and security.[76] AI-powered code-generation tools enable technical and non-technical users to build software using natural language, with the North American market projected to grow from $700 million to $4 billion by 2030.[77] While these tools aid the DIB by accelerating software development, they pose risks if threat actors exploit them.

AI strengthens cybersecurity by analyzing vast data sets to detect threats missed by traditional systems, offering pattern recognition, actionable recommendations, and autonomous mitigation.[78] It's essential in protecting intellectual property, detecting supply chain anomalies, and monitoring maritime threats like AIS spoofing.[79]

AI improves logistics through predictive maintenance and scenario planning to mitigate disruptions. Experts note that AI enhances situational awareness by analyzing data from global sources to identify emerging risks. Beyond defense, AI advances fields like medicine and climate science while improving operational efficiency and innovation.

Risks and Challenges

Despite its advantages, AI introduces security vulnerabilities. AI code generators frequently produce insecure code, with studies showing that 40% of GitHub Copilot's outputs contained critical weaknesses, and ChatGPT generated secure code for only 5 of 21 programs tested. [80] [81] Threat actors can poison training data from platforms like GitHub and HuggingFace, leading to

[76] Marcus Law, "'Magnificent Seven' Tech Companies Driving Forward With AI," *Technology Magazine*, February 20, 2024, https://technologymagazine.com/articles/magnificent-seven-tech-companies-driving-forward-with-ai.
[77] "North America AI Code Generator Market Trends: Understanding the Future," LinkedIn, accessed April 15, 2025, https://www.linkedin.com/pulse/north-america-ai-code-generator-market-trends-understanding-dryme/.
[78] Lampis Alevizos and Martijn Dekker, "Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline," Electronics 13, no. 11 (2024):1, https://doi.org/10.3390/electronics13112021.
[79] Navya Chandrika, "Artificial Intelligence in Maritime Security," *The International Prism*, September 13, 2022, https://www.theinternationalprism.com/artificial-intelligence-in-maritime-security/.
[80] Hammond Pearce, Baleegh Ahmad, Benjamin Tan, Brendan Dolan-Gavitt, and Ramesh Karri, "Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions," arXiv, August 2021, http://export.arxiv.org/pdf/2108.09293.
[81] Raphael Khoury, Anderson R. Avila, Jacob Brunelle, and Baba Mamadou Camara, "How Secure is Code Generated by ChatGPT?," arXiv, April 19, 2023,

compromised AI models (see Figure 1).[82] These corrupted models may be further exploited via indirect prompt injections, compounding cyber risks.

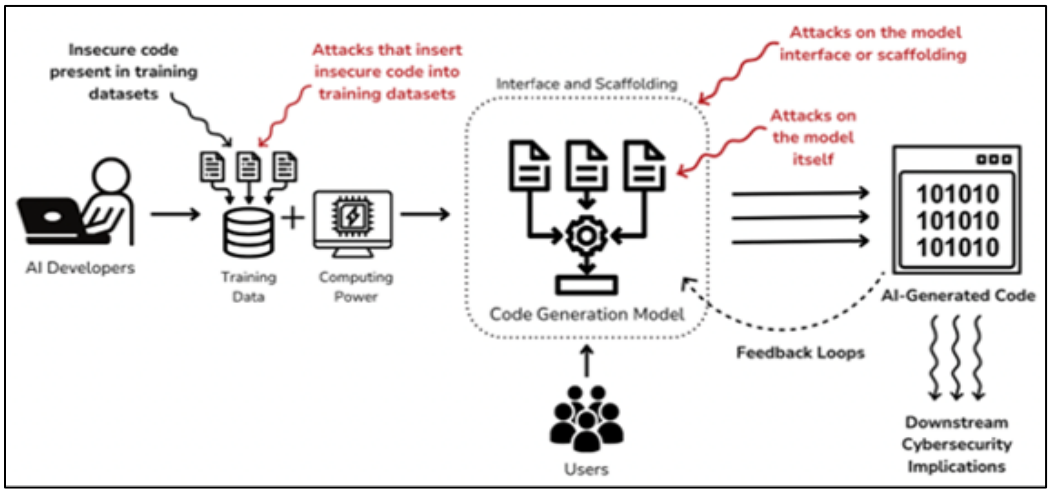

Figure 1: AI Code-Generation Development and Threat Attack Types

APTs from nations like China, Russia, North Korea, and Iran, over 57 tracked groups, are incorporating AI into their operations, from malware creation to reconnaissance.[83] The fusion of AI and disinformation is particularly dangerous because it enables scalable manipulation of public trust. AI's ability to generate persuasive misinformation makes it a potent tool for adversaries, especially in sensitive sectors like maritime transport.[84] Regulatory gaps persist, particularly in military AI applications. While the EU's AI Act aims to govern ethical AI, its military exclusion leaves room for unchecked risk.[85] As AI accelerates international competition and reshapes defense strategies, it raises concerns about proliferation, instability, and governance.

[82] Jessica Ji, Jenny Jun, Maggie Wu, and Rebecca Gelles, "Cybersecurity Risks of AI-Generated Code," Center for Security and Emerging Technology, November 2024, 12.
[83] "Google: Over 57% of Nation-State Threat Actors Use Commercial Spyware," The Hacker News, January 30, 2025, https://thehackernews.com/2025/01/google-over-57-nation-state-threat.html
[84] Craig H. Allen Jr., "The Coast Guard Must Prepare for AI-Enhanced Disinformation," U.S. Naval Institute,
[85] "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)."

Appendix B: Integration of Information and Cyberspace in Wargaming

Key Players, Roles, and Responsibilities:

- Joint Force Development and Design Center (JS J-7) coordinates broad joint wargaming and experimentation activities. It collaborates closely with OSD, combatant commands, the defense industrial base, academia, and research centers through federated frameworks like the Joint Experimentation Affiliate Network (JExNet).[86]
- Cyber Command and the National Defense University lead targeted cyber defense simulations and training.
- CISA often leads in bridging the public-private divide. CISA offers free tools, training, and resources to government organizations and private industry. CISA also offers complete exercise packages and supports tailored exercise development and conduct.[87]
- Academic Institutions: Public and private academic institutions often lead innovation and the development of theoretical constructs.
- Private Sector: Companies like Optiv Security provide cyber strategy consulting and integration; Amazon Web Services hosts large-scale simulation platforms.[88] Other tech giants and data management firms offer various cybersecurity consulting services.
- Think Tanks & NGOs: Atlantic Council, Center for Naval Analyses, MITRE, and others provide expertise, analysis, and neutral assessment environments.[89]
- Defense Industrial Base: Engages directly in simulations, notably GridEx, to ensure critical infrastructure resilience.[90]
- National Infrastructure Sectors: The United States identifies 16 critical infrastructure sectors. These should be regular participants in war games related to cyber threats.

Critical Requirements for Cyber-Threat Wargames:

- Clearly Defined Objectives: Essential for targeting specific educational or research goals.
- Realistic Scenarios: Incorporate relevant political, military, and economic contexts.
- Technically Accurate: High-fidelity digital twins of the network, systems, and infrastructure.
- Participant Diversity: Including government, military, and private sector stakeholders.

---

[86] MG Lew Irwin, "Joint War Gaming & Experimentation" (PowerPoint Presentation, National Defense University, October 23, 2019).
[87] "Cybersecurity Training & Exercises | CISA," accessed April 30, 2025, https://www.cisa.gov/cybersecurity-training-exercises.
[88] Frank L. SmithIII, Nina A. Kollars, and Benjamin H. Schechter, *Cyber Wargaming : Research and Education for Security in a Dangerous Digital World* (Washington: Georgetown University Press, 2024), https://research.ebsco.com/linkprocessor/plink?id=023b1412-3c3c-397c-af7c-c03cd80a9ea5.
[89] David B. Fox et al., "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," *Homeland Security Systems Engineering & Development Institute*, no. 18–1636 (August 29, 2018).
[90] Frank L. Smith III, Nina A. Kollars, and Benjamin H. Schechter, *Cyber Wargaming : Research and Education for Security in a Dangerous Digital World*.

    - Leadership: Understand capabilities, limitations, and decision authorities.
    - Technical Experts: Ensure realism and set expectations.
    - Strategy and Policy Experts: Align inputs and outputs to real-world needs.
- Thorough Analysis: Rigorous methods ensure realistic outcomes and valuable insights.
- Repetition and Adaptability: Repeated exercises to test different scenarios and adaptive response capabilities under varied conditions.
- Shared Threat Intelligence: Communication between private cybersecurity firms and government agencies to develop wargame threats and scenarios.

Existing Wargame Gaps

- Limited Integration: Insufficient incorporation of cyber operations in exercises across physical domains.
- Inconsistent Realism: Difficulty accurately capturing dynamic, real-time complexities of cyber environments and threats in synthetic scenarios.
- Fragmentation in Leadership: Lack of centralized authority and unified strategy to guide cohesive responses. Adversaries exploit seems and gray zones between government entities and private industry.
- Reluctance in Private Sector Cooperation: Privacy and shareholder value impart high thresholds for private sector organizations to seek government assistance.

Recommendations to Improve Wargaming

- Enhanced Integration: Incorporate cyber realism and cybersecurity scenarios into kinetic wargames (e.g., JADC2) to test real-world impacts across physical and cyber domains.
- Expanded Participation: Increase and incentivize the involvement of industry stakeholders and allied nations to build global cyber resilience.
- Leveraging Digital Twins: Use advanced digital twin simulations to replicate real network environments and evaluate potential vulnerabilities and response strategies.[91]
- Composite Wargames: Merging tabletop strategic decision-making games with realistic red-team exercises to capture tactical and strategic dimensions.
- Specialized Scenarios: Explicitly simulating critical cyberattacks against command-and-control infrastructure and critical civilian systems to test national resilience.
- Eliminate Fragmented Authorities: Bridging the public-private domains requires deliberate prescriptive legal authorities to mitigate threats as they traverse from overseas to domestic, between government and private systems, and across industries with inconsistent regulation.
- Joint Scenario Development: Develop, plan, and test joint exercises with public and private entities to capture the interests and equities of all stakeholders.
- Mutual Aid and Response Agreements: Establish predefined processes for public assistance during private-sector cyber crises (Privateers and private sector mobilization)

[91] Rajive Bagrodia, "Using Network Digital Twins to Improve Cyber Resilience of Missions," n.d.