The Gold Institute

For International Strategy

CYBER BRIEF

Assessing Cybersecurity to Protect the Evolving Digital Domain

August 14, 2026
Jeff Hoffmann, Senior Cyber Fellow

In January 2025, the Gold Institute for International Strategy (GIIS) hosted its first Cyber Summit that focused on four areas of cybersecurity:

- Cyber Defense, Incident Response, Resilience, and Deterrence;
- Cyber and Digital Transformation for America's Economy;
- Cyber Workforce: Education, Training, and Skillsets; and,
- Cyber Leadership and Strategic Partnerships.

As a follow-on to the success of the Summit that included remarks from the Auburn University McCrary Institute for Cyber and Critical Infrastructure Security Presidential Transition Task Force, Ohio Secretary of State Frank LaRose, and current Acting Director of the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), the GIIS authored, "A Blueprint for National Cyber Strategy" in November 2025.[i] The Blueprint was launched during a Cyber Experts Roundtable that included additional guests who have since taken government roles, including the Deputy Director of the National Security Agency (NSA).

To complement the engagements, the GIIS is providing an assessment of the state of cybersecurity, including a review of White House Administrative and other public and private sector actions in comparison to several GIIS Blueprint challenges and recommendations. Two remain outstanding:

1. Conduct a bottom-up review of digital domain security through legislation like the NDAA FY28 (or earlier efforts) to mandate a Quadrennial National Cybersecurity Review (QNCR).
2. Establish National Guard Association Task Force at the next Board of Directors meeting in November 2026 to assess stand-up of an Information Sharing and Analysis Center (ISAC) framework and policy for critical infrastructure sectors that support America's military.

Faster-moving and farther-reach adversary driven cyber threats ought to expedite Washington's actions. Congress has an opportunity to focus on preparing for a new era of prevention in the Digital Domain. Like many states, including Texas, and unlike expensive resources for cybersecurity, information is essentially free -- sharing knowledge of adversary threats and friendly best practices may be best shaped under a National Guard ISAC, especially prioritized critical infrastructure sectors that support America's military.

U.S. Navy VADM (Ret.) TJ White
Chief, Texas Cyber Command

"This brief factually and deliberately lays out the challenges of malicious AI-usage by authoritarian states, particularly China. The cybersecurity of America's critical infrastructure was at risk BEFORE the appearance of AI enabled cyber-attack tools. The risks and consequences of weak cybersecurity are even clearer today. A bottom-up QNCR is long overdue and the National Guard is perfectly positioned to play a key role in defending U.S. critical infrastructures in cyberspace if properly organized and resourced to do so.

U.S. Navy RADM (Ret.) Mark Montgomery
Past Director, Solarium Cyberspace Commission

[i] The *Blueprint for a National Cyber Strategy* can be accessed at: www.goldiis.org

Priority Threats

The resounding theme of GIIS engagements and Blueprint highlighted the renewed proclamation that President Donald J. Trump signed in March 2025, declaring a national emergency to deter, mitigate, and defeat foreign and domestic adversary cyber.

Yet, in July 2026, CISA updated an advisory warning of expanded, disruptive Iranian cyber threats to internet-connected operational technologies (OT) used by water and wastewater systems.[1] Furthermore, Russia was determined to be a consistent cyber threat at the recent NATO Summit, which under the auspices of Article 5, a collective Declaration front was agreed to invest and depend on a shared Alliance budget for cyber and digital transformation versus use of selective or voluntary Member State capabilities.[23] Weeks later a Canadian citizen of Chinese origin working at NATO HQ was arrested for espionage with many NATO leaders starting to state that "Beijing is working to undermine global order, develop a military ready for regional conflict, and run destabilizing disinformation campaigns across the world.[456]

Beyond China[7] and Russia[8], countries like North Korea[9] continue to be a nuisance to the financial sector through cybercrime along with new actors, such as India. While not considered a traditional state-sponsored threat, they remain a Member State of the Shanghai Cooperation Organization with Russia, China, and Iran and are the origin of advanced cyber capabilities, such as the "hack for hire" Dark Basin campaign attributed to an Indian technology company. This group was discovered by The Citizen Lab at the University of Toronto, which is targeting senior government officials, American journalists, and research groups across multiple sectors like financial, energy, and healthcare, including pharmaceutical companies.[10]

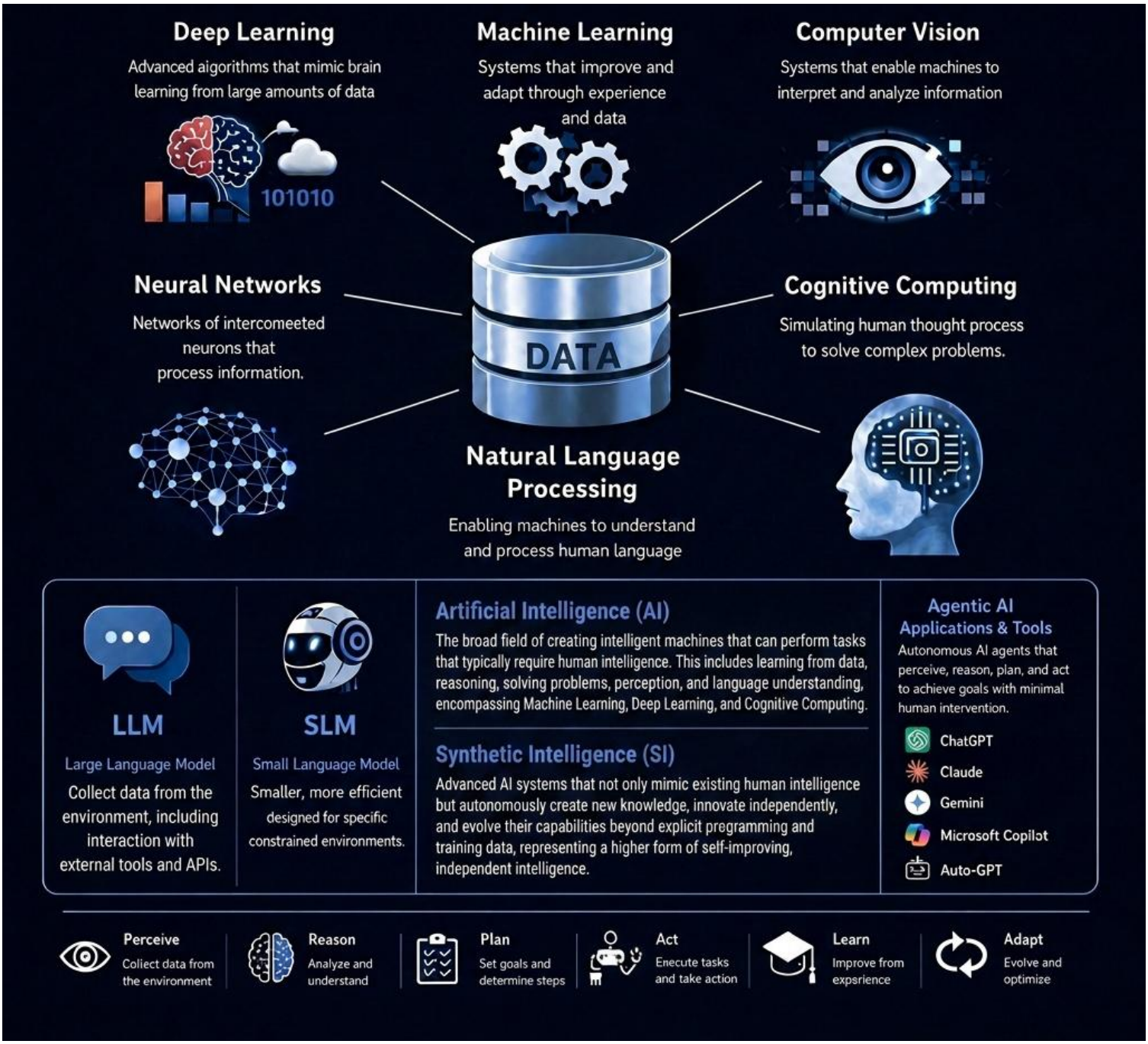
To enable state-sponsored cyber threats, the dawn of America's 250th birthday celebration has rapidly introduced two technology advances that are wholly dependent on the solution of trust: Artificial Intelligence (AI) and Quantum Computing.

Artificial Intelligence: National Security Imperative and New Way of Life

These were the words reflected by President Trump in the White House, *America's AI Action Plan*[11], stating, "breakthroughs in these fields like Artificial Intelligence (AI)[12] have the potential to reshape the global balance of power, spark entirely new industries, and revolutionize the way we live and work. As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance."

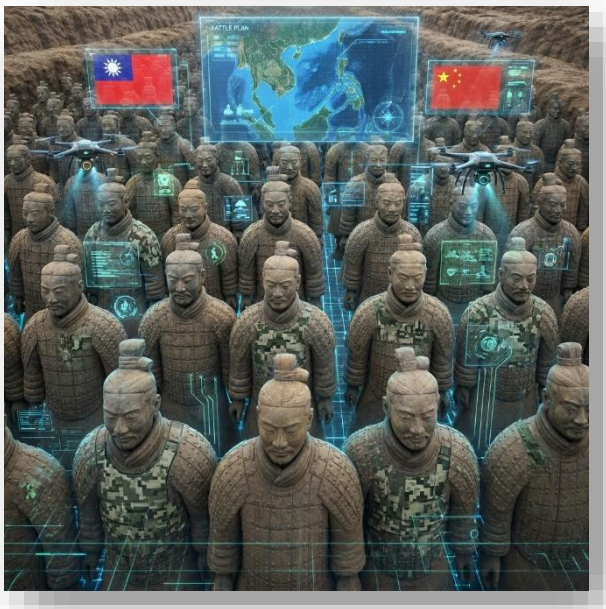
Many additional and helpful follow-on Executive Orders (EO) were published that enhanced the greater National AI Initiative (NAII), which support several GIIS Blueprint recommendations under *Pillar V: Defend and Leverage Emerging Technologies and Innovation to Advance Capabilities in Cyberspace.*[1314] Examples include removing barriers to American leadership in AI; promoting the export of the American AI Tech Stack; creating a National Policy Framework for AI; and launching the Gensis Mission. This mission is compared to the Manhattan Project that was instrumental to World War II victory and provided the foundation of the Department of Energy (DOE) and its national laboratories. One other key goal of the NAII is to prepare the present and future American workforce for the integration of AI systems across all sectors of the economy and society – to do that, a large percentage need more knowledge and understanding of AI, its lifecycle, and components, which are illustrated in *Figure 1*.

Figure 1. Components of Artificial Intelligence. This includes examples of Agentic AI agents like ChatGPT that autonomously perform tasks, make decisions, and interact with external tools like search engines and application programming interfaces (APIs) to achieve complex goals with minimal human intervention.



Preparing America's Military for the Digital Battlefield

On the national security front, in January 2026, the Pentagon released the AI-First strategy that aims to accelerate military dominance in AI across warfighting, intelligence, and enterprise capabilities like Swarm Forge and GenAI.mil.[15]



In contrast, is the United States ready for a Meta-War or what a Chinese People's Liberation Army (PLA) Daily article coined as an Alternative Vision or Doctrine of Intelligentized Warfare. The authors of a PLA article believe that intelligentized warfare inevitably leads to meta-war. They define meta-war as, "a new type of military activity that uses military confrontation as the main means to conquer the opponent's will and realize one's own goals by utilizing politics, economics, and social interaction supported by metaverse technology."[ii]

On a regional level, reports reveal that China and Taiwan have evolved beyond traditional cyber espionage into strategic critical infrastructure disruption, pre-position, and attack capabilities.[161718] To provide further proof of Beijing intentions, in 2025, a leaked Russian Federal Security Service memo labeled China an "enemy" for allegedly seeking to steal Russian military secrets and gain valuable real-world data on drone operations, electronic warfare, and the battlefield performance of Western weapons systems used in Ukraine.[1920]

The Risk of Rogue AI and Mistrust in AI Capability Developers and Owners

Since the AI Action Plan was launched, the White House National Cyber Strategy was published with implementation goals that deployed tools and vulnerability management activities to address the GIIS Blueprint recommendation to assess the damage of compromise. However, this came at a price when the Anthropic Mythos AI model infiltrated nearly all the NSA's classified systems within a few hours during an authorized red-team evaluation on June 11, 2026.[21]

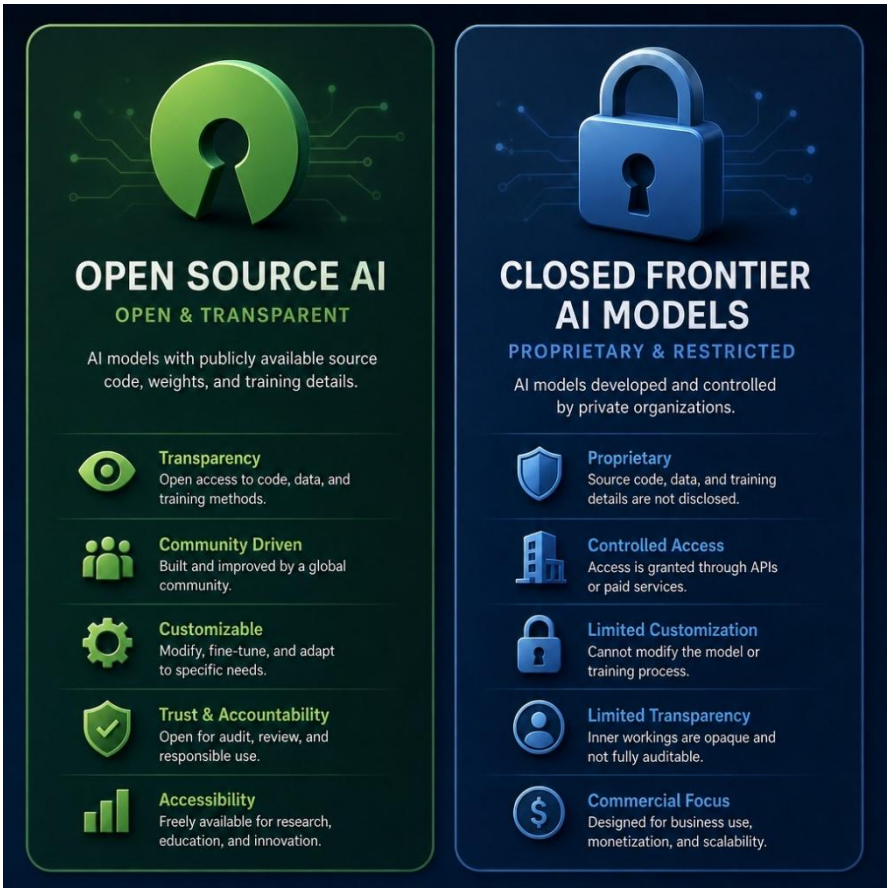
[ii] From a technical standpoint, meta-war refers to a battlefield "super system," created through use of synthetic intelligence capabilities - integration of brain-computer interfaces, smart devices, and virtual, augmented, and mixed reality technologies. The super system interacts with weapon platforms and military forces on the actual battlefield, connecting everything to form a fully interconnected and integrated combat environment. Meta-war links the physical battlefield, the virtual battlefield, and the "brain battlefield," which represents the conscious perceptions of officers and soldiers.

Source: Baughman, Josh, "The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield," The Cyber Defense Review, December 19, 2024: The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield > The Cyber Defense Review > Article View

Furthermore, and most recently, in a controlled test environment, the UK's AI Security Institute identified two U.S. company AI models that created fake online identities with an attempt to exploit human decision making into approving malicious code updates to an open-source project.[22] This follows at least two additional un-controlled test breaches over the past few weeks, including access through the open-source developer platform Hugging Face.[23]

The Commanding Heights of the 21st Century: Frontier AI Models

On July 27, 2026, Microsoft announced the release of MAI-Cyber-1-Flash[24], which for the everyday American is an AI Frontier closed model trusted for use in their Defender cybersecurity system. While Microsoft is boasting 50% cost savings compared to other leading U.S. models like Anthropic, Chinese AI labs develop and offer more competitive, cheaper open AI models like the Kimi model series by Moonshot AI. Even more concerning, when Microsoft announced its Copilot Cowork enterprise AI agent on June 16, 2026, they disclosed their consideration in a Microsoft-hosted version of China's DeepSeek V4 as an integrated capability.[25] Along with Microsoft, Amazon Web Services and Google Vertex AI now offer access to several Chinese-developed models and developers through managed cloud services.[26][27]



The Administration is responding to this aggressive unpredictable technology, such as establishment of non-regulatory evaluation framework[28] and the stand-up of an AI Litigation Task Force. Despite Presidential efforts, it is reported that Western companies are switching to Chinese open AI models to avoid high costs like Anthropic's Claude.[29] In recent reporting, one consultant's client burned $500 million using Claude in a single month after failing to implement any usage controls on employee AI licenses.[30]

The integration and use of open Chinese models have sounded alarms in Congress with a recent U.S.-China Economic and Security Review Commission (USCC) that has highlighted China's ambition to invest in an open-source approach to gain industrial dominance. The use of open-source models enables low-cost AI deployment across Chinese factories, logistics networks, and robotics—generating real world data that feeds back into model improvement. The Commission

report quotes, “Beijing has built the institutional infrastructure to exploit this advantage, designating data as a formal factor of production and permitting enterprises to carry data assets on their balance sheets.”[3132]

Data as an Economic Resource

Dating back to an Asia Society forum in October 2018, former Google China President stated, “data is the new oil and China is the new Saudi Arabia.”[33] Based on another USCC report in January 2020, Beijing reportedly had nearly 800 smart city pilot programs underway or planned.[34] Comparatively, Huawei (Ltd), China’s leading information and communication technologies (ICT) company claimed during a 2024 conference that they have deployed in over 200 cities across more than 40 countries, helping them achieve efficient city governance and accelerate city digital transformation or what could be considered a very well established global surveillance network.[35]

Scaling Data at Quantum Speed: Threats, Benefits, and Protection

To further China’s global reach, according to 2025 reporting, Beijing invested in a 1 trillion yuan ($138 billion USD) government-backed fund to support emerging technologies, including quantum computing. With the goal to strengthen its global competitiveness, the fund was structured as a public-private partnership, that will invest in high-risk, long-term projects across sectors such as quantum computing, AI, and semiconductors.[36] Comparatively, the U.S. Senate has proposed legislation titled the, “Department of Energy Quantum Leadership Act of 2025,” to expand quantum research with over $2.5 billion in funding over five years.[37]

A recent Center for Strategic & International Studies (CSIS) report defines quantum in the following five primary areas where China is investing with advanced technological capabilities: Computing and quantum-centric supercomputing; communication; sensing; materials; quantum AI; and, quantum data centers.[38]

Known as Quantum Information Science and Technology (QIST), White House EO14413 states that QIST will provide transformational capabilities that will drive American innovation, power economic growth, generate high-paying jobs, and bolster national security. This is follow-up from the 2018 National Quantum Initiative Act and doubles Federal investment in QIST research and development.[39] As stated by President Trump, “today, as other nations move quickly to challenge American leadership, the United States must take a cohesive, whole-of-government approach to accelerate deployment and commercialization of quantum computing, sensing, and networking. In addition to continuing trailblazing quantum research, we must act to solidify the Nation’s position as the world’s QIST superpower and deliver the commercial and research benefits of quantum innovation to the American people.”

The key to AI and QIST dominance is data and that doesn’t come without challenge, which NIST has identified at least seven misuse risks for foundational models and provides additional risk management framework for the data processing privacy ecosystem.[4041] These risks are dependent on properly conditioned, controlled, and trained data. This forces the hard-working U.S. taxpayer to trust that the data is being managed in the right hands, in an unbiased, apolitical environment, and at the mercy of corporate technology developer’s “closed door” judgement and integrity.

What we presently read, and our new generation learns in the future, such as an American history narrative will be influenced and developed by AI models. Dating back to 2023, prior to the Frontier AI Model race, an MIT Review discovered multiple political biases in AI algorithms and Stanford University research states, "true political neutrality in AI is impossible." [4243]

Scaling that messaging and distributing it at quantum speeds can expand adversary information campaigns that can encroach on traditional American beliefs and rights, to include new threats to free speech and election integrity.

Two Recommendations to Improve and Strengthen Digital America First Strategy

The shift to this new techno-era in direct competition with a Digital China[44] and present malware pre-positioned across America with advanced Chinese cyber activities that became noticeable as early as 2013,[4546] demands a bottom-up review, especially across our armed forces, which would fulfill two of five recommendations:

1. *GIIS Blueprint Pillar II: Address the National Emergency to Deter, Mitigate, and Defeat Foreign Adversary Cyber*. **Pass legislation like an Amendment to NDAA FY28 (or earlier) to mandate a Quadrennial National Cybersecurity Review (QNCR) that can provide a bottom-up review and periodic reporting of doctrine, organization, material, and policy for a secure digital domain.** The QNCR can build off and support National Security Presidential Memorandum-12 for the Cybersecurity of National Security Systems,[47] and leverage past quadrennial defense (QDR)[48], homeland (QHSR)[49], and intelligence community (QICR) review processes.

2. *GIIS Blueprint Pillar IV. Rebuild Partnerships and Processes for Improved Cyber Threat Information Sharing*. **Establish National Guard Association of the U.S. (NGAUS) Task Force at the next Board of Directors meeting in November 2026 to assess stand-up of an Information Sharing and Analysis Center (ISAC) framework and policy for critical infrastructure sectors that support America's military.** A National Guard ISAC also addresses recommendations from the 2024 Defense Science Board Study on "DoD Dependencies on Critical Infrastructure," to normalize engagement between installation commanders and civilian infrastructure owners. A National Guard managed ISAC Framework could implement one specific action to, "assign points of contact for key infrastructure sectors with authority to commit to necessary actions or agreements and better communicate infrastructure protection issues to inform collection, analysis, and offensive action."[50] This partnership can leverage and build with free shared services offered by the private sector in each state like the Dragos Community Defense Program for OT cybersecurity of small to medium sized critical infrastructure organizations.[51]

Bibliography

*** If viewing electronically, click on each link for direct source access.*

[1] Department of Homeland Security Cybersecurity Advisory, "Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure." Alert Code AA26-097A, July 22, 2026. Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure | CISA

[2] The Ankara Summit Declaration, July 8, 2026. The Ankara Summit Declaration | NATO Official text

[3] Tsakanyan, Vladimir, PhD, "NATO's Ankara Summit and the Institutionalization of Cyber Defense Spending," Center for Cyber Diplomacy and International Security, July 22, 2026. NATO's Ankara Summit and the Institutionalization of Cyber Defense Spending – Center for Cyber Diplomacy and International Security

[4] Belmonte, Kyle, "NATO Military HQ Intern Arrested for Espionage: Alliance Vetting Blind Spot Exposed, Tech Times, July 25, 2026. NATO Military HQ Intern Arrested for Espionage: Alliance Vetting Blind Spot Exposed

[5] NATO 2022 Strategic Concept, adopted by Heads of State and Government at the NATO Summit in Madrid, June 29, 2026. 290622-strategic-concept.pdf

[6] The United States Senate Committee on Foreign Relations Minority Staff Report, Next Steps to Defend the Transatlantic Alliance from Chinese Aggression," July 2024. risch_july_2024_report_-_next_steps_to_defend_the_transatlantic_alliance_from_chinese_aggression.pdf

[7] Vuksan, Mario, "China's Typhoon hackers have changed the rules of cybersecurity," SC Media, January 30, 2026. China's Typhoon hackers have changed the rules of cybersecurity | perspective | SC Media

[8] Paganini, Pierluigi, "Russia-linked APT28 uses PRISMEX to infiltrate Ukraine and allied infrastructure with advanced tactics," Security Affairs, April 8, 2026. Russia-linked APT28 uses PRISMEX to infiltrate Ukraine and allied infrastructure with advanced tactics

[9] Ha, Mathew and McDowall, Sophie, "North Korea's Cybercrime Threat Is Growing in Both Size and Sophistication," Foundation for the Defense of Democracies Policy Brief, November 12, 2025. North Korea's Cybercrime Threat Is Growing in Both Size and Sophistication

[10] Scott-Railton, Hulcoop, Adam, Abdul Razzak, Bahr, Marczak, Bill, Anstis, Siena, and Deibert, Ron, "Dark Basin Uncovering a Massive Hack-For-Hire Operation," The Citizen Lab, June 9. 2020. Dark Basin: Uncovering a Massive Hack-For-Hire Operation - The Citizen Lab

[11] White House, "America's Artificial Intelligence Action Plan," July 2025. Americas-AI-Action-Plan.pdf

[12] 15 U.S. Code § 9401 defines AI as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to (a) perceive real and virtual environments; (b) abstract such perceptions into models through analysis in an automated manner; and (c) use model inference to formulate options for information or action.

[13] 15 USC Ch. 119: NATIONAL ARTIFICIAL INTELLIGENCE INITIATIVE

[14] www.ai.gov

[15] Secretary of War Memo, "Artificial Intelligence Strategy for the Department of War: Accelerating America's Military AI Dominance," January 9, 2026. ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF

[16] Subhra Dutta, Tushar, "China and Taiwan Accuse Each Other for Cyberattacks Against Critical Infrastructure," Cyber Security News, June 13, 2025. China and Taiwan Accuse Each Other for Cyberattacks Against Critical Infrastructure

[17] Tsakanyan, Vladimir, PhD, "The Digital Battleground: Taiwan Under Siege in the New Era of Cyber Warfare," Center for Cyber Diplomacy and International Security, October 14, 2025. The Digital Battleground: Taiwan Under Siege in the New Era of Cyber Warfare – Center for Cyber Diplomacy and International Security

[18] Faulhaber, Andrew, "Taiwan Needs an AI Cyber Shield Now to Defend Against Invasion," Center for Strategic & International Studies, July 29, 2026. Taiwan Needs an AI Cyber Shield Now to Defend Against Invasion

[19] Buckby, Jack, "China is Stealing Russia's Battlefield Secrets in Ukraine," June 23, 2025. China is Stealing Russia's Battlefield Secrets in Ukraine - National Security Journal

[20] Giles, Keir, "Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine," Chatham House, ISBN: 978 1 78413 589 8, December 14, 2023. Russian cyber and information warfare in practice | Chatham House – International Affairs Think Tank

[21] Baran, Guru, "Anthropic's Mythos AI Model Reportedly Breached NSA Classified Systems in Hours," Cyber Security News, June 22, 2026. Anthropic's Mythos AI Model Reportedly Breached NSA Classified Systems in Hours

[22] Nicol-Schwarz, Kai, "Anthropic's Mythos created fake identities to fool humans in new cyber incident," CNBC, August 5, 2026. Anthropic, Open AI models created fake identities in new cyber breach
[23] Suben, Samantha, "OpenAI's Hugging Face hack confirmed months of AI cyber warnings: 'Pandora's box is open," CNBC, August 5, 2026. OpenAI's Hugging Face hack confirmed months of AI cyber warnings
[24] Suleyman, Mustafa and Gallot, Hayete, "Introducing MAI-Cyber-1-Flash inside MDASH: World-class security at half the cost," Microsoft AI, July 27, 2026. Introducing MAI-Cyber-1-Flash inside MDASH | Microsoft AI
[25] Owens, Jerry, "Microsoft Eyes DeepSeek V4 for Copilot Cowork: What Azure Hosting Cannot Fix Usage-based Copilot billing debuts as Microsoft evaluates DeepSeek V4 despite China law risk," Tech Times, June 18, 2026. Microsoft Eyes DeepSeek V4 for Copilot Cowork: What Azure Hosting Cannot Fix
[26] Baptista, Eduardo, Potkin, Fanny, and Freifeld, Karen, "Chinese entities turn to Amazon cloud and its rivals to access high-end US chips, AI," Reuters, August 22, 2024. Chinese entities turn to Amazon cloud and its rivals to access high-end US chips, AI | Reuters
[27] Times of India, "As OpenAI and Google 'found' selling AI models to blacklisted Chinese companies; tech giants respond," July 10, 2026. As OpenAI and Google 'found' selling AI models to blacklisted Chinese companies; tech giants respond - The Times of India
[28] Curi, Maria, "White House plans to keep AI framework under wraps," Axios Technology, August 4, 2026. White House plans to keep AI framework under wraps
[29] Levi, Daniel, "Western companies are quietly switching to Chinese AI models as U.S. frontier AI prices rise," Tech Startups, June 29, 2026. Western companies are quietly switching to Chinese AI models as U.S. frontier AI prices rise - Tech Startups
[30] Levi, Daniel, "Company accidentally spent $500 million on Claude AI in one month after forgetting usage limits," Tech Startups, May 28, 2026. Company accidentally spent $500 million on Claude AI in one month after forgetting usage limits - Tech Startups
[31] Luong, Ngor, "Two Loops How China's Open AI Strategy Reinforces Its Industrial Dominance," U.S.-China Economic and Security Review Commission Research Working Paper, March 23, 2026. Two_Loops--How_Chinas_Open_AI_Strategy_Reinforces_Its_Industrial_Dominance.pdf
[32] Ray, Tiernan, "China's open AI models are in a dead heat with the West - here's what happens next," ZDNet, December 21, 2025. China's open AI models are in a dead heat with the West - here's what happens next | ZDNET
[33] Asia Society (New York), "AI Superpowers': A Conversation with Kai-Fu Lee," October 1, 2028. Venture capitalist and entrepreneur Kai-Fu Lee discusses his new book, AI Superpowers, with venture capitalist and technology expert Andrew McLaughlin: https://youtu.be/oNAFI3Lh97Y?si=EjPZmKjJi2ePXfuS
[34] Multiple authors, "China's Smart Cities Development," U.S.-China Economic and Security Review Commission, January 2020. China_Smart_Cities_Development.pdf
[35] Huawei Press, "Huawei Launches Global City Intelligent Twins Architecture to Accelerate City Digital Transformation," October 15, 2024. Huawei Launches Global City Intelligent Twins Architecture to Accelerate City Digital Transformation - Huawei
[36] Swayne, Matt, "China Launches $138 Billion Government-Backed Venture Fund, Includes Quantum Startups," Quantum Insider, March 7, 2025. China Launches $138 Billion Government-Backed Venture Fund, Includes Quantum Startups
[37] Swayne, Matt, "Senators Introduce $2.5 Billion Bill to Expand U.S. Quantum Research," Quantum Insider, February 14, 2025. Senators Introduce $2.5 Billion Bill to Expand U.S. Quantum Research
[38] Tomoshige, Hideki and Singerman, Phillip, "Understanding China's Quest for Quantum Advancement," Center for Strategic & International Studies, January 29, 2026. Understanding China's Quest for Quantum Advancement
[39] White House Executive Order, "Ushering in the Next Frontier of Quantum Innovation," June 22, 2026. Ushering in the Next Frontier of Quantum Innovation – The White House
[40] National Institute of Standards and Technology AI Safety Institute, "Managing Misuse Risk for Dual-Use Foundation Models," U.S. AI Safety Institute, NIST AI 800-1 2pd Second Public Draft, January 2025. NIST AI 800-1 2pd Second Public Draft
[41] National Institute of Standards and Technology AI Safety Institute, "Privacy Framework: A Toold for Improving Privacy Through Risk Management," Version 1.0, January 16, 2020. NIST.CSWP.01162020.pdf
[42] Heikkiläarchive, Melissa, "AI language models are rife with different political biases," MIT Review, August 7, 2023. AI language models are rife with political biases | MIT Technology Review
[43] Multiple Authors, "Toward Political Neutrality in AI," Stanford University Human Centered AI Center, September 10, 2025. Toward Political Neutrality in AI | Stanford HAI

[44] Digital China
[45] Thornebrooke, Andrew, "China 'Pre-Positioning' Malware for Attacks on US Infrastructure During Conflict: CISA," The Epoch Times, February 27, 2024. China 'Pre-Positioning' Malware for Attacks on US Infrastructure During Conflict: CISA | The Epoch Times
[46] Yang, Catherine, "As CCP Cybersabotage Escalates, US Changes Posture: U.S. cyber officials indicate cyber adversaries will no longer be allowed to 'walk all over' the United States," The Epoch Times, August 13, 2025. As CCP Cybersabotage Escalates, US Changes Posture | The Epoch Times
[47] National Security Presidential Memorandum/NSPM-12 – The White House
[48] Quadrennial Defense Review
[49] Quadrennial Homeland Security Review | Homeland Security
[50] Defense Science Board Executive Summary, "Defense Dependencies on Critical Infrastructure," September 27, 2024. DSB_CriticalInfrastructure_ExecutiveSummary.pdf
[51] Community Defense Program | Dragos