U.S. House Committee on Energy and Commerce
Subcommittee on Energy
"Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid."
December 2, 2025
Documents for the Record

1. Letter from Members of the U.S. House of Representative addressed to Secretary of Commerce Howard Lutnick, submitted by Rep. Balderson and Rep. Pfluger.
2. Letter from the Digital Power Network (DPN) addressed to Chairman Guthrie and Chairman Latta, submitted by the Majority.
3. Letter from the American Public Power Association addressed to Chairman Latta, Ranking Member Castor, Chairman Guthire, and Ranking Member Pallone, submitted by the Majority.
4. A report from ANTHROP\C titled "Disrupting the first reported AI-orchestrated cyber espionage campaign", submitted by the Majority.
5. An article from Utility Dive titled "As cyber threats grow, utilities say lapsed information-sharing law stymies security", submitted by the Majority.
6. A report from the Office of the Director of National Intelligence titled "Annual Threat Assessment of the U.S. Intelligence Community", submitted by the Majority.
7. An article from the Wall Street Journal titled "FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale", submitted by the Majority.
8. An article from the Wall Street Journal titled "The First Large-Scale Cyberattack by AI", submitted by the Majority.
9. Letter from Beam Global addressed to Chairman Latta and Ranking Member Castor, submitted by the Majority.

Congress of the United States
House of Representatives
Washington, DC 20515-0906

November 14, 2025

The Honorable Howard Lutnick
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Dear Secretary Lutnick,

We write to express our deep concern regarding the growing risks to the United States electric grid posed by technologies designed, programed, and manufactured by adversarial nations. We urge the Department of Commerce to act swiftly to safeguard our grid and energy infrastructure from Chinese-made critical grid components and energy technologies that pose a severe threat to the safety of our constituents. As we work to achieve President Trump's vision of American energy dominance, it is vital that our critical infrastructure is not dependent on technologies that could be exploited to undermine U.S. national security.

The integration of critical grid technologies, such as utility-scale solar and battery inverters, sourced from foreign entities of concern pose unacceptable national security, economic, and supply chain risks. This is especially true as the United States faces historic electricity demand growth due to the AI revolution, new data centers, and increased industrial manufacturing places unprecedented strain on our grid. According to the Department of Energy's 2025 Resource Adequacy Report, expected retirements of existing generation capacity coupled with projected load growth increases the risk of power outages in 2030 by 100 times.

Earlier this year, a Reuters investigation revealed that certain Chinese-manufactured solar and batteries inverters deployed across the nation contained undisclosed communication devices. Experts warn that these "rogue" components could bypass firewall protections and enable malicious remote access, potentially allowing adversaries to destabilize large portions of the grid. Simultaneously, a growing body of Chinese academic research reveals a systematic and technically advanced focus on how to hack, harm, or even collapse Western power grids, particularly through the exploitation of Chinese-made technologies embedded in American grid infrastructure, including through the use of inverters. Increasing our reliance on China for inverters and critical grid equipment is a mistake, especially as we have ample supply domestically and from allied nations that would not expose our national security to unacceptable risks.

For these reasons, we respectfully request that the Department of Commerce exercise its authorities to restrict the future importation of such Chinese equipment and inverters for U.S. critical infrastructure. Such action would also align with the Trump Administration's broader objectives of strengthening domestic supply chains and protecting American workers and consumers. We appreciate your attention to this matter, and we stand ready to work with you and your team to ensure the security and resilience of our grid.

Respectfully,

August Pfluger
Member of Congress

Ben Cline
Member of Congress

Troy Balderson
Member of Congress

Zach Nunn
Member of Congress

Randy Weber
Member of Congress

James Moylan
Member of Congress

Jodey C. Arrington
Member of Congress

Roger Williams
Member of Congress

H. Morgan Griffith
Member of Congress

Bob Latta
Member of Congress

Richard Hudson
Member of Congress

Buddy Carter
Member of Congress

Gary Palmer
Member of Congress

Dan Crenshaw
Member of Congress

Rick Allen
Member of Congress

Russ Fulcher
Member of Congress

Jay Obernolte
Member of Congress

Cliff Bentz
Member of Congress

Laurel Lee
Member of Congress

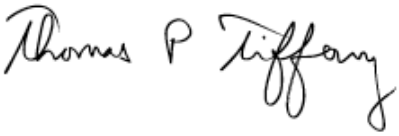
Craig Goldman
Member of Congress

Tracey Mann
Member of Congress

Mike Haridopolos
Member of Congress

Julie Fedorchak
Member of Congress

Jake Ellzey
Member of Congress



Thomas Tiffany
Member of Congress

Bill Huizenga
Member of Congress

Brian Babin
Member of Congress

Dan Newhouse
Member of Congress

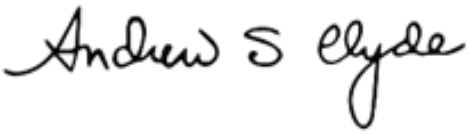
Rich McCormick
Member of Congress

Barry Loudermilk
Member of Congress

Pat Fallon
Member of Congress

William Timmons
Member of Congress

Austin Scott
Member of Congress



Andrew Clyde
Member of Congress

Ann Wagner
Member of Congress

Stephanie Bice
Member of Congress

Andy Barr
Member of Congress

Adrian Smith
Member of Congress

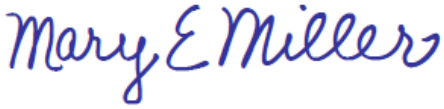
Scott Fitzgerald
Member of Congress

Scott Franklin
Member of Congress

Marlin A. Stutzman
Member of Congress

David Rouzer
Member of Congress

Rudy Yakym
Member of Congress



Mary Miller
Member of Congress

Michael Cloud
Member of Congress

W. Gregory Steube
Member of Congress

Brad Finstad
Member of Congress

Joe Wilson
Member of Congress

John J. McGuire III
Member of Congress

Sheri Biggs
Member of Congress

Pat Harrigan
Member of Congress

Jeff Hurd
Member of Congress

Jefferson Shreve
Member of Congress

Abraham Hamadeh
Member of Congress

Addison McDowell
Member of Congress

DIGITAL POWER NETWORK

December 2, 2025

Energy & Commerce Subcommittee on Energy
2125 Rayburn House Office Building
Washington, DC 20515-6116

Dear Chairman Guthrie, Chairman Latta, and Members of the Subcommittee,

Thank you for the opportunity to submit this letter regarding the Energy and Commerce Subcommittee on Energy's hearing titled "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid." The Digital Power Network (DPN) is the largest coalition of Bitcoin miners and digital infrastructure providers, representing over 85% of the U.S. public Bitcoin mining hashrate. DPN advocates for policies that promote energy innovation, grid resilience, economic development, and the strategic role of digital assets in the 21st-century economy.

As the Subcommittee evaluates how to mitigate physical and cyber risks from foreign adversaries to our nation's infrastructure, data center security should be a central focus. The United States currently hosts nearly 40% of global Bitcoin mining hashrate, a position that enables meaningful regulatory oversight and downstream economic benefits. Bitcoin miners supply computing power that secures the network and protects trillions in digital assets worldwide. As Bitcoin and AI operations increasingly converge, these facilities are strengthening transmission resilience.

While AI has been recognized by both the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Permitting Improvement Steering Council as critical or covered infrastructure, Bitcoin mining has largely been excluded from these discussions despite its close relationship to AI computing. Bitcoin mining and its related operations are foundational to U.S. energy systems, both because miners are diversifying into AI and because of the unique energy characteristics and grid benefits associated with Bitcoin facilities. Federal recognition of cryptocurrency operations as critical infrastructure is therefore a national security imperative.

Bitcoin data centers have also emerged as distinctive grid-balancing resources capable of rapidly adjusting power consumption to support electric reliability. These facilities can curtail operations within minutes in response to grid stress, effectively functioning as on-call

reserve capacity. Bitcoin mining contributes to national energy security by encouraging new domestic energy development and making the grid more flexible and sustainable. Miners can monetize stranded or otherwise wasted energy resources– such as flared, curtailed, or unused power– and instantly reduce consumption when that energy is needed elsewhere. As energy markets increasingly incorporate mechanisms that reward flexible loads, miners have become more fully integrated into the foundation of the grid.

Bitcoin miners also further enhance national cybersecurity by contributing to a more decentralized computing and operational landscape. Decentralization is a long-standing security model for national infrastructure and a core principle of Bitcoin. It not only secures digital assets but also provides a physical and operational model for strengthening critical energy systems. Just as gold reserves are geographically dispersed to limit systemic risk, distributed generation and computing resources reduce vulnerabilities by minimizing exposure to localized disruptions. This architecture decreases regional overreliance and strengthens resilience to both cyber and physical threats, ensuring that essential digital and energy systems remain robust amid evolving risks.

With more than 5,000 major data centers in the United States, Bitcoin miners help form an integral part of the backbone of the internet, cloud computing, and the digital economy. Although data centers are not designated as a standalone sector within the CISA framework, they clearly fall within the Information Technology and Communications sectors and are widely recognized as essential to the economy and national security. Bitcoin mines function as high-density computing centers, contributing to the security of a global financial network (Bitcoin) and offering valuable services to the energy grid. They occupy a unique position at the intersection of the Energy Sector and the IT/Cyber Sector, both of which are among the 16 federally recognized critical infrastructure sectors.

The Cybersecurity and Infrastructure Security Agency Act of 2018 created CISA and designated it as the primary oversight body for the nation's critical infrastructure. The Act mandates the development of national plans to secure "power production, generation, and distribution systems; information technology and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency communications systems; and the physical and technological assets that support those systems." While CISA has relied on this directive to guide its work on AI infrastructure security, it is critical that all forms of data center operations, including Bitcoin mining, be recognized as critical infrastructure and incorporated into federal security frameworks.

DIGITAL POWER NETWORK

Beyond CISA, the Fixing America's Surface Transportation (FAST)-41 framework has also played a significant role in supporting energy and data center development by improving federal permitting efficiency. Delays in permitting threaten the United States' ability to maintain a strong domestic data center presence by slowing the deployment of energy and transmission projects, as well as delaying manufacturing buildout and interconnection for digital infrastructure. In 2022, FAST-41 was amended to include semiconductors, artificial intelligence and machine learning, high-performance computing and advanced hardware, quantum information science, data storage and management, and cybersecurity. This amendment was a major step toward securing efficient data center growth in the U.S., but FAST-41 should be further amended to include Bitcoin operations, both mining and manufacturing. Doing so will ensure policy alignment across the digital infrastructure industry and support appropriate federal oversight and recognition of both Bitcoin and AI.

As the Subcommittee on Energy looks to bolster the security of the nation's critical infrastructure, it is essential to recognize the key role that Bitcoin miners and related data center operations play in supporting national energy resilience, cybersecurity, and economic competitiveness. Ensuring that these facilities are appropriately included within federal critical infrastructure frameworks, including CISA designations and FAST-41 permitting, will strengthen U.S. leadership in digital infrastructure while improving the reliability, flexibility, and security of the electric grid. DPN appreciates the Subcommittee's attention to these issues and stands ready to serve as a resource as Congress continues its work to safeguard America's energy systems.

Sincerely,

Digital Power Network

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

December 1, 2025

The Honorable Bob Latta
Chairman
Subcommittee on Energy
House Energy & Commerce Committee
2470 Rayburn House Office Building
Washington, DC 20515

The Honorable Kathy Castor
Ranking Member
Subcommittee on Energy
House Energy & Commerce Committee
2188 Rayburn House Office Building
Washington, DC 20515

The Honorable Brett Guthrie
Chairman
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Frank Pallone
Ranking Member
House Energy & Commerce Committee
2323 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Latta, Ranking Member Castor, Chairman Guthrie, and Ranking Member Pallone:

The American Public Power Association (APPA) appreciates the opportunity to submit this letter ahead of the hearing before the House Energy & Commerce Committee's Energy Subcommittee titled, "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid."

APPA is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. APPA represents public power before the federal government to protect the interests of the more than 55 million people that public power utilities serve in 49 states and five territories, and the 100,000 people they employ. Public power utilities account for 15 percent of all sales of electric energy (kilowatt-hours) to end-use consumers and are load-serving entities with the primary goal of providing the communities they serve with safe and reliable electric service at the lowest reasonable cost. This orientation aligns the interests of the utilities with the long-term interests of the residents and businesses in their communities

Public power utilities know that a reliable energy grid is the lifeblood of the nation's economic and national security, as well as vital to the health and safety of all Americans and take very seriously their responsibility to maintain a secure and reliable electric grid. The key pillars of cyber and physical security (collectively known as "grid security") are 1) mandatory and enforceable standards, 2) information sharing and protection, 3) public private partnerships, and 4) "defense-in-depth" and sector-wide preparation exercises. These pillars are detailed in APPA's attached "issue brief." For purposes of this statement, APPA would like to focus on the need to reauthorize the Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program (RMUC).

Enacted in 2021, RMUC Program was authorized to appropriate a total of $250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. APPA believes that the program is a generational opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities that should be extended and expanded.

Through RMUC, APPA has received a four-year, $4 million cooperative agreement to establish the Cyber Pathways program. This program is designed to support public power utilities with cybersecurity assessments, training, and a new cybersecurity designation program to recognize utilities implementing cybersecurity best practices. Cyber Pathways has a particular focus on resource-limited public power utilities, to connect them with cybersecurity resources and improve their cyber maturity and incident response capabilities.

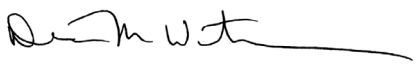
The program has notched several successes, such as the completion of a legal framework for utility cybersecurity assessment data, a report on cybersecurity frameworks in use by public power utilities, and steady progress developing the Cybersecurity Accelerator Program (CAP) designation but has also been delayed by funding uncertainties in the first half of 2025, communication restrictions on Department of Energy staff, and slow contract approvals.

APPA has also applied for additional funding under the DE-FOA-0002986 Advanced Cybersecurity Technology (ACT) Funding Opportunity Announcement. APPA's proposal for Topic Area 3 – Increasing Access to Technical Assistance and Training for Utilities with Limited Cybersecurity Resources, would award $2 million over four years to improve cybersecurity incident response capabilities at 19 utilities that agreed to participate. However, delays and reassessments of program priorities and spending at the Office of Cybersecurity, Energy Security, and Emergency Response have put award decisions and finalizations on hold.

RMUC is authorized through 2026. Given the slow rollout, a substantial amount of funding remains and, as such, APPA strongly supports extending the availability of existing funds to 2030. APPA also believes that targeted changes to the program's authorizing language can be made to increase the efficiency of disbursing funds and would welcome a discussion on how best to do that.

Thank you for the opportunity to comment. We look forward to working with the subcommittee on this important issue.

Sincerely,



Desmarie Waterhouse
Senior Vice President, Advocacy and Communications & General Counsel
The American Public Power Association

AMERICAN PUBLIC POWER ASSOCIATION
Powering Strong Communities

ISSUE BRIEF June 2025

Grid Security

- The electric sector has mandatory and enforceable federal regulatory standards in place for cyber and physical security (collectively known as grid security).
- Close coordination among industry and government partners at all levels is imperative to deterring attacks and preparing for emergency situations.
- Congress should expeditiously reauthorize the Cybersecurity and Information Security Act of 2015 (CISA 2015) to ensure that the legal structure for the voluntary sharing of information between and among the federal government and private entities remains in place.
- Congress should postpone consideration of legislation to create additional cyber incident reporting mandates for the energy sector until the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) is fully implemented.

Background – The Key Pillars of Grid Security

Mandatory and Enforceable Standards

Congress approved the mandatory and enforceable standards regulatory regime for the bulk power system in the Energy Policy Act of 2005 (EPAct05) (section 215 of the Federal Power Act (FPA)). Under section 215, the North American Electric Reliability Corporation (NERC), working with electric industry experts, regional entities, and government representatives, regularly drafts reliability, physical security, and cybersecurity standards that apply across the North American grid, including Canada. Participation by industry experts and compliance personnel in the NERC critical infrastructure protection (CIP) standards development process ensures that the standards are technically sound, fair, and balanced. The Federal Energy Regulatory Commission (FERC) has the power to approve or remand those standards as they apply in the United States. To ensure compliance, under FERC's oversight, NERC and its regional entities conduct rigorous audits and can levy substantial fines for non-compliance. Additionally, FERC can instruct NERC to develop new or revised reliability standards with a very short turn-around time. CIP standards establish an important baseline of security—but they are a floor, not a ceiling—and grid security is and should be much more than a compliance exercise.

Information Sharing and Protection

The electric sector is unique in that it has long been subject to cyber incident reporting mandates to the Department of Energy (DOE) via an Electricity Emergency Incident and Disturbance Report (OE-417) and NERC/FERC. Moreover, there is robust electric utility industry participation in information sharing organizations known as the Electricity Information Sharing and Analysis Center (E-ISAC) and the Multi-State Information Sharing and Analysis Center.

Another layer of mandatory cyber incident sharing requirements will be added through CIRCIA. Signed into law in March 2022, CIRCIA will require covered critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In March 2024, CISA released a notice of proposed rulemaking (NOPR) to begin implementing CIRCIA. APPA is concerned that the

NOPR is overbroad with respect to reporting requirements for small, distribution-only electric utilities. While reporting obligations are appropriate for large utilities that serve millions of customers, it is unnecessary and burdensome to impose the same obligation on hundreds of community-owned electric utilities that serve fewer than 2,000 customers each and pose a negligible risk to the reliability of the broader grid. APPA is also concerned that CISA is moving forward with its rule without having finalized plans and agreements to avoid duplicative reporting requirements. Prior to issuing a final rule, APPA believes that CISA should complete its consultations with DOE and FERC and enter an information sharing agreement with them.

The ability to protect sensitive electric information from public disclosure is critical to grid security. The Fixing America's Surface Transportation Act of 2015 or "FAST Act" (Sec. 61003 of P.L. 114-94) gave the Secretary of Energy broader authority to address grid security emergencies under the FPA and clarified the ability of FERC and other federal agencies to protect sensitive critical electric infrastructure information (CEII) from public disclosure under the Freedom of Information Act and other sunshine laws. Under the FAST Act, CEII is exempted from disclosure for a period of up to five years with a process to lift the designation or challenge it in court. In addition, it established sanctions for the unauthorized disclosure of shared information. It is critical to operational security that the industry is confident that sensitive information about critical infrastructure that might provoke new threats or endanger the integrity of the electric power grid is not publicized. CEII in the public sphere creates a grave vulnerability to the electric power grid by significantly reducing the surveillance effort required by dedicated domestic and foreign adversaries. APPA has supported legislation and actions by DOE and FERC that would further clarify and enhance the responsibility of the federal government and other stakeholders to maintain the confidentiality of CEII to minimize the risk that such information could be used by malicious actors to target grid infrastructure.

Finally, CISA 2015 set up policies and procedures for voluntary sharing of cybersecurity threat information between and among the federal government and private entities (the definition of which includes public power utilities) and provides limited liability protection for these activities.

Public-Private Partnerships

The electric power industry works closely with the federal government, including NERC, FERC, DOE, and DHS, on matters of critical infrastructure protection. One important venue for this collaboration is the Electricity Subsector Coordinating Council (ESCC). The ESCC serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for, and respond to, national-level disasters or threats to critical infrastructure. APPA and public power utilities play a leadership role on the ESCC, which includes utility CEOs and trade association leaders representing all segments of the industry. Their counterparts include senior administration officials from the White House, relevant Cabinet agencies, federal law enforcement, and national security organizations.

APPA works closely with DOE on several fronts. Notably, APPA has been awarded four grants since 2016 to help strengthen the cybersecurity posture of public power utilities. APPA is currently executing a grant of $15 million over eight years from DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to facilitate the adoption and deployment of industrial control systems cybersecurity technologies for municipal utilities. This builds off an existing $6 million, seven-and-a-half-year cooperative agreement (awarded in 2020) to develop and deploy cyber and cyber-physical solutions for public power utilities, and a previous three-year cooperative agreement (awarded in 2016) to assist small- and medium-sized public power utilities with cyber risk assessment and cybersecurity training.

The Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance (RMUC) Program, which passed as part of the Infrastructure Investment and Jobs Act (P.L. 117-58), is based off the successes of these grant programs. The RMUC Program is authorized to appropriate a total of $250 million in grants and technical assistance over five years to rural, municipal, and small investor-owned electric utilities to enhance their security posture. In 2024, APPA was awarded a $4 million grant to launch the Cyber Pathways program to improve the cybersecurity posture of public power utilities with limited resources, serving military installations, or are critical to the bulk-power system. President Trump's fiscal year 2026 budget request proposes to rescind $166.1 million in unobligated RMUC funds. APPA believes that the program is a generational opportunity to improve the cybersecurity of under-resourced, not-for-profit utilities and that the proposal to rescind funds is unwarranted.

"Defense-in-Depth" and Sector-Wide Preparation Exercises

The goal of every utility and the entire industry is to manage risk prudently. Still, there are tens of thousands of diverse facilities throughout the U.S. and Canada that cannot be protected 100 percent of the time from all threats, requiring utilities to prioritize

facilities and assets that, if damaged, would have the most severe impacts on their ability to keep the power on. As such, the electric power industry employs threat mitigation known as "defense-in-depth" that focuses on preparation, prevention, response, and recovery to "all hazard" threats to electric grid operations.

Electric utilities plan and regularly exercise for a variety of emergency situations that could impact their ability to provide electricity. One of the biggest exercises, GridEx, takes place every two years. Managed by NERC and the E-ISAC, GridEx VII will take place this November and will involve hundreds of organizations and thousands of participants from industry, government agencies, and partners in Canada and Mexico.

Building off the success of GridEx, APPA will host its first ever cyber mutual aid exercise, Safe Haven, in fall 2025, funded by DOE. Safe Haven will be held in Washington and Kansas, locations that were selected in coordination with DOE based on several criteria. The scenario will feature a cyber event that has physical impacts to the grid. APPA is working in close coordination with the E-ISAC to help drive participation by smaller utilities that do not usually participate in GridEx and to provide them with lessons learned to incorporate into the biennial exercise.

The three primary segments of the electric utility industry—public power, investor-owned, and rural electric cooperatives—have long had in place mutual aid response networks to share employees and resources to restore power after natural disasters and other emergencies. The ESCC used the concept of traditional mutual assistance networks to develop the Cyber Mutual Assistance program that can help electric and natural gas companies, public power utilities, and/or rural electric cooperatives restore critical computer systems following significant cyber incidents. The program now includes 200 entities across all segments of the industry, serving more than 85 percent of all U.S. electric customers.

Finally, electric utilities regularly share transformers and other equipment through long existing bilateral and multilateral sharing arrangements and agreements. The industry is expanding equipment sharing programs—like the Spare Transformer Equipment Program, SpareConnect, and Grid Assurance—to improve grid resiliency.

Congressional Action

In May 2025, Senators James Lankford (R-OK) and Gary Peters (D-MI) introduced S. 1875, the Streamlining Federal Cybersecurity Regulations Act. The bill would establish an interagency Harmonization Committee at the Office of the National Cyber Director (ONCD), which is housed in the White House, and would require the committee to develop a framework for the alignment of cybersecurity and information security regulations, rules and compliance requirements. It would also require that all agencies, including independent regulatory agencies, consult with the committee before issuing or updating regulations. APPA strongly supports the goals of the bill.

As noted above, CISA 2015 set up policies and procedures for the voluntary sharing of cybersecurity threat information between and among the federal government and private entities and provided limited liability protection for these activities. The law will expire on September 30, and APPA is part of a coalition of critical infrastructure sectors advocating for the law's extension. Senators Mike Rounds (R-SD) and Gary Peters (D-MI) have introduced legislation (S. 1337) to extend CISA 2015 for ten years; APPA strongly supports S. 1337.

APPA Contacts

Amy Thomas, Vice President of Government Relations, 202-467-2934 / athomas@publicpower.org

Michael Coe, Vice President of Physical and Cyber Security Programs, 202-467-2956 / mcoe@publicpower.org

The American Public Power Association is the voice of not-for-profit, community-owned utilities that power 2,000 towns and cities nationwide. We represent public power before the federal government and protect the interests of the more than 55 million people that public power utilities serve and the 100,000 people they employ.

ANTHROP\C

Disrupting the first reported AI-orchestrated cyber espionage campaign

Full report

November 2025

Changelog

November 17, 2025

- Updated language in the Executive Summary (p.3) to clarify our high confidence in our attribution of the espionage operation.

Executive summary

We have developed sophisticated safety and security measures to prevent the misuse of our AI models. While these measures are generally effective, cybercriminals and other malicious actors continually attempt to find ways around them. This report details a recent threat campaign we identified and disrupted, along with the steps we've taken to detect and counter this type of abuse. This represents the work of Threat Intelligence: a dedicated team at Anthropic that investigates real world cases of misuse and works within our Safeguards organization to improve our defenses against such cases.

In mid-September 2025, we detected a highly sophisticated cyber espionage operation. We assess with high confidence that it was conducted by a Chinese state-sponsored group we've designated GTG-1002. It represents a fundamental shift in how advanced threat actors use AI. Our investigation revealed a well-resourced, professionally coordinated operation involving multiple simultaneous targeted intrusions. The operation targeted roughly 30 entities and our investigation validated a handful of successful intrusions.

Upon detecting this activity, we immediately launched an investigation to understand its scope and nature. Over the following ten days, as we mapped the severity and full extent of the operation, we banned accounts as they were identified, notified affected entities as appropriate, and coordinated with authorities as we gathered actionable intelligence.

This campaign demonstrated unprecedented integration and autonomy of AI throughout the attack lifecycle, with the threat actor manipulating Claude Code to support reconnaissance, vulnerability discovery, exploitation, lateral movement, credential harvesting, data analysis, and exfiltration operations largely autonomously. The human operator tasked instances of Claude Code to operate in groups as autonomous penetration testing orchestrators and agents, with the threat actor able to leverage AI to execute 80-90% of tactical operations independently at physically impossible request rates.

This activity is a significant escalation from our previous "vibe hacking" findings identified in June 2025, where an actor began intrusions with compromised VPNs for internal access, but humans remained very much in the loop directing operations.

GTG-1002 represents multiple firsts in AI-enabled threat actor capabilities. The actor achieved what we believe is the first documented case of a cyberattack largely executed without human intervention at scale—the AI autonomously discovered vulnerabilities in targets selected by human operators and successfully exploited them in live operations, then performed a wide range of post-exploitation activities from analysis, lateral movement, privilege escalation, data access, to data exfiltration. Most significantly, this

marks the first documented case of agentic AI successfully obtaining access to confirmed high-value targets for intelligence collection, including major technology corporations and government agencies. While we predicted these capabilities would continue to evolve, what has stood out to us is how quickly they have done so at scale.

An important limitation emerged during investigation: Claude frequently overstated findings and occasionally fabricated data during autonomous operations, claiming to have obtained credentials that didn't work or identifying critical discoveries that proved to be publicly available information. This AI hallucination in offensive security contexts presented challenges for the actor's operational effectiveness, requiring careful validation of all claimed results. This remains an obstacle to fully autonomous cyberattacks.

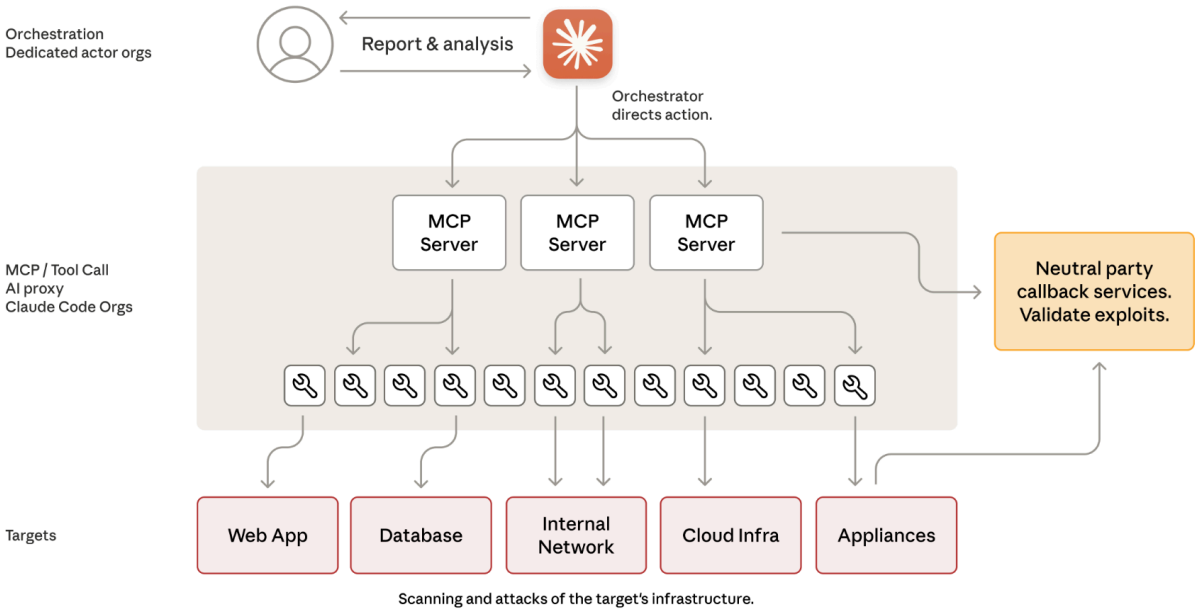
While we only have visibility into Claude usage, this case study likely reflects consistent patterns of behavior across frontier AI models and demonstrates how threat actors are adapting their operations to exploit today's most advanced AI capabilities. Rather than merely advising on techniques, the threat actor manipulated Claude to perform actual cyber intrusion operations with minimal human oversight.

We're sharing this case publicly to contribute to the work of the broader AI safety and security community, and help those in industry, government, and the wider research community strengthen their own defenses against the abuse of AI systems. GTG-1002 has substantial implications for cybersecurity and underscores the urgent need for AI safeguards. We plan to continue releasing reports like this regularly, and to be transparent about the threats we find.

A general-language summary of this report can be found at this link.

Contents

Simplified architecture diagram of the operation



Operational infrastructure

The threat actor developed an autonomous attack framework that used Claude Code and open standard Model Context Protocol (MCP) tools to conduct cyber operations without direct human involvement in tactical execution. The framework used Claude as an orchestration system that decomposed complex multi-stage attacks into discrete technical tasks for Claude sub-agents—such as vulnerability scanning, credential validation, data extraction, and lateral movement—each of which appeared legitimate when evaluated in isolation. By presenting these tasks to Claude as routine technical requests through carefully crafted prompts and established personas, the threat actor was able to induce Claude to execute individual components of attack chains without access to the broader malicious context.

The architecture incorporated Claude's technical capabilities as an execution engine within a larger automated system, where the AI performed specific technical actions based on the human operators' instructions while the orchestration logic maintained attack state, managed phase transitions, and aggregated results across multiple sessions. This approach allowed the threat actor to achieve operational scale typically associated with nation-state campaigns while maintaining minimal direct involvement, as the framework autonomously progressed through reconnaissance, initial access, persistence, and data exfiltration phases

by sequencing Claude's responses and adapting subsequent requests based on discovered information.

AI-driven autonomous operations with human supervision

The operational model represents a fundamental departure from traditional AI assistance patterns. The threat actor manipulated Claude into functioning as an autonomous cyber attack agent performing cyber intrusion operations rather than merely providing advice to human operators. Analysis of operational tempo, request volumes, and activity patterns confirms the AI executed approximately 80 to 90 percent of all tactical work independently, with humans serving in strategic supervisory roles.

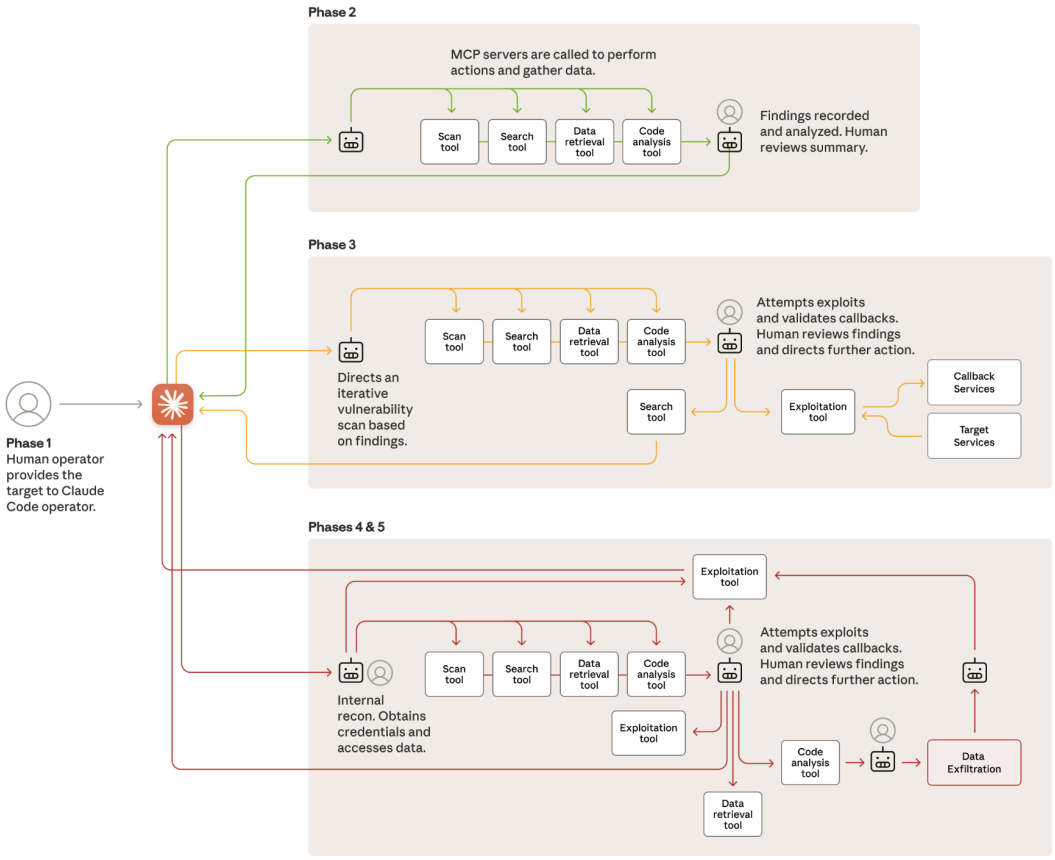
Human operators maintained minimal direct engagement, estimated at 10 to 20 percent of total effort. Human responsibilities centered on campaign initialization and authorization decisions at critical escalation points. Human intervention occurred at strategic junctures including approving progression from reconnaissance to active exploitation, authorizing use of harvested credentials for lateral movement, and making final decisions about data exfiltration scope and retention.

The AI component demonstrated extensive autonomous capability across all operational phases. Reconnaissance proceeded without human guidance, with the threat actor instructing Claude to independently discover internal services within targeted networks through systematic enumeration. Exploitation activities including payload generation, vulnerability validation, and credential testing occurred autonomously based on discovered attack surfaces. Data analysis operations involved the AI parsing large volumes of stolen information to independently identify intelligence value and categorize findings. Claude maintained persistent operational context across sessions spanning multiple days, enabling complex campaigns to resume seamlessly without requiring human operators to manually reconstruct progress.

The operational tempo achieved proves the use of an autonomous model rather than interactive assistance. Peak activity included thousands of requests, representing sustained request rates of multiple operations per second. The substantial disparity between data inputs and text outputs further confirms the AI actively analyzed stolen information rather than generating explanatory content for human review.

Attack lifecycle and AI integration

The campaign proceeded through structured phases where AI autonomy increased progressively while human oversight remained concentrated at strategic decision gates.



Phase 1: Campaign initialization and target selection

Human operators began campaigns by inputting a target. The framework's orchestration engine would then task Claude to begin autonomous reconnaissance against multiple targets in parallel. Initial targets included major technology corporations, financial institutions, chemical manufacturing companies, and government agencies across multiple countries. At this point they had to convince Claude—which is extensively trained to avoid harmful behaviors—to engage in the attack. The key was role-play: the human operators claimed that they were employees of legitimate cybersecurity firms and convinced Claude that it was being used in defensive cybersecurity testing. Eventually, the sustained nature of the attack triggered detection, but this kind of "social engineering" of the AI model allowed the threat actor to fly under the radar for long enough to launch their campaign.

AI role: Minimal direct involvement during initialization. Human strategic direction predominates.

Phase 2: Reconnaissance and attack surface mapping

Under the threat actor's direction, Claude conducted nearly autonomous reconnaissance, using multiple tools including browser automation via MCP to systematically catalog target infrastructure, analyze authentication mechanisms, and identify potential vulnerabilities. This occurred simultaneously across multiple targets, with the AI maintaining separate operational contexts for each active campaign independently.

Discovery activities proceeded without human guidance across extensive attack surfaces. In one of the limited cases of a successful compromise, the threat actor induced Claude to autonomously discover internal services, map complete network topology across multiple IP ranges, and identify high-value systems including databases and workflow orchestration platforms. Similar autonomous enumeration occurred against other targets' systems with the AI independently cataloging hundreds of discovered services and endpoints.

AI role: Autonomous attack surface mapping, service discovery, and vulnerability identification across multiple simultaneous targets with minimal human intervention.

Phase 3: Vulnerability discovery and validation

Exploitation proceeded through automated testing of identified attack surfaces with validation via callback communication systems. Claude was directed to independently generate attack payloads tailored to discovered vulnerabilities, execute testing through remote command interfaces, and analyze responses to determine exploitability.

Example: Vulnerability discovery and exploitation sequence

Claude's autonomous actions (1-4 hours)	**Human operator actions (2-10 minutes)**
Task 1: Discovery • Scans target infrastructure • Enumerates services and endpoints • Maps attack surface Task 2: Vulnerability Analysis • Identifies SSRF vulnerability • Researches exploitation techniques	

Task 3: Exploit Development • Authors custom payload • Develops exploit chain • Validates exploit capability via callback responses • Generates exploitation report Task 4: Exploit Delivery • Deploys exploit for initial access • Establishes foothold in environment Task 5: Post-Exploitation • Enumerates internal services • Identifies admin interfaces • Discovers metadata endpoints	→ Reviews AI findings and recommendations → Approves exploitation

When sufficient evidence existed for the exploitation phase, the AI documented comprehensive findings for human review at authorization gates.

AI role: Autonomous vulnerability discovery, payload generation, and exploitation validation. Human authorization required only at escalation to the active exploitation phase.

Phase 4: Credential harvesting and lateral movement

Upon receiving authorization from the human operators, Claude executed systematic credential collection across targeted networks. This involved querying internal services, extracting authentication certificates from configurations, and testing harvested credentials across discovered systems. Claude independently determined which credentials provided access to which services, mapping privilege levels and access boundaries without human direction.

Lateral movement proceeded through AI-directed enumeration of accessible systems using stolen credentials. Claude systematically tested authentication against internal APIs, database systems, container registries, and logging infrastructure, building comprehensive maps of internal network architecture and access relationships.

AI role: Autonomous credential extraction, testing, and lateral movement with self-directed targeting based on discovered infrastructure. Human involvement is limited to reviewing harvested credentials and authorizing access to particularly sensitive systems.

Phase 5: Data collection and intelligence extraction

Collection operations demonstrated the most extensive AI autonomy. Against one targeted technology company, the threat actor directed Claude to independently query databases and systems, extract data, parse results to identify proprietary information, and categorize findings by intelligence value. Similar autonomous data processing occurred across other compromises, where the AI extracted user credentials, system configurations, and sensitive operational data without detailed human direction.

Example: Database extraction operation

Claude's autonomous actions (2-6 hours)	**Human operator actions (5-20 minutes)**
1. Authenticate with harvested credentials	
2. Map database structure and query user account tables	
3. Extract password hashes and account details	
4. Identify high-privilege accounts	
5. Create persistent backdoor user account	
6. Download complete results to local system	
7. Parse extracted data for intelligence value	
8. Categorize by sensitivity and utility	
9. Generate summary report	→ Reviews AI findings and recommendations → Approves final exfiltration targets

The AI processed large volumes of data identifying valuable intelligence automatically rather than requiring human analysis.

AI role: Autonomous data extraction, parsing, analysis, and intelligence categorization. Human review occurred only at the final exfiltration approval stage.

Phase 6: Documentation and handoff

Claude automatically generated comprehensive attack documentation throughout all campaign phases. Structured markdown files tracked discovered services, harvested credentials, extracted data, exploitation techniques, and complete attack progression. This documentation enabled seamless handoff between operators, facilitated campaign resumption after interruptions, and supported strategic decision-making about follow-on activities.

Evidence suggests the threat actor handed off persistent access to additional teams for sustained operations after initial intrusion campaigns achieved their intelligence collection objectives.

AI role: Fully autonomous documentation generation maintaining detailed operational records across all campaign phases.

Technical sophistication

The operational infrastructure relied overwhelmingly on open source penetration testing tools rather than custom malware development. Standard security utilities including network scanners, database exploitation frameworks, password crackers, and binary analysis suites comprised the core technical toolkit. These commodity tools were orchestrated through custom automation frameworks built around Model Context Protocol servers, enabling the framework's AI agents to execute remote commands, coordinate multiple tools simultaneously, and maintain persistent operational state.

The custom development of the threat actor's framework focused on integration rather than novel capabilities. Multiple specialized servers provided interfaces between Claude and various tool categories:

- Remote command execution on dedicated penetration testing systems
- Browser automation for web application reconnaissance
- Code analysis for security assessment
- Testing framework integration for systematic vulnerability validation
- Callback communication for out-of-band exploitation confirmation

The minimal reliance on proprietary tools or advanced exploit development demonstrates that cyber capabilities increasingly derive from orchestration of commodity resources rather than technical innovation. This accessibility suggests potential for rapid proliferation across the threat landscape as AI platforms become more capable of autonomous operation.

Our response

Upon discovering this attack, we banned the relevant accounts and implemented multiple defensive enhancements in response to this campaign.

This investigation prompted a significant response from Anthropic. We expanded detection capabilities to further account for novel threat patterns, including by improving our cyber-focused classifiers. We are prototyping proactive early detection systems for autonomous cyber attacks and developing new techniques for investigating and mitigating large-scale distributed cyber operations.

We notified relevant authorities and industry partners, and shared information with impacted entities where appropriate. This attack pattern has been incorporated into our broader safety and security controls, informing both technical defensive systems and cyber harm policy frameworks.

Cybersecurity implications

This campaign demonstrates that the barriers to performing sophisticated cyberattacks have dropped substantially—and we can predict that they'll continue to do so. Threat actors can now use agentic AI systems to do the work of entire teams of experienced hackers with the right set up, analyzing target systems, producing exploit code, and scanning vast datasets of stolen information more efficiently than any human operator. Less experienced and less resourced groups can now potentially perform large-scale attacks of this nature.

This attack is an escalation even on the "vibe hacking" findings we reported this summer: in those operations, humans were very much still in the loop, directing the operations. Here, human involvement was much less frequent, despite the larger scale of the attack. And while our visibility is limited to Claude usage, this case study likely reflects consistent patterns of behavior across frontier AI models and demonstrates how threat actors are adapting their operations to exploit today's most advanced AI capabilities.

This raises an important question: if AI models can be misused for cyberattacks at this scale, why continue to develop and release them? The answer is that the very abilities that allow Claude to be used in these attacks also make it crucial for cyber defense. When sophisticated cyberattacks attacks inevitably occur, our goal is for Claude—into which we've built strong safeguards—to assist cybersecurity professionals to detect, disrupt, and prepare for future versions of the attack. Indeed, our Threat Intelligence team used Claude extensively in analyzing the enormous amounts of data generated during this very investigation.

But having these capabilities available isn't enough on its own. The cybersecurity community needs to assume a fundamental change has occurred: Security teams should experiment with applying AI for defense in areas like SOC automation, threat detection, vulnerability assessment, and incident response and build experience with what works in their specific environments. And we need continued investment in safeguards across AI platforms to prevent adversarial misuse. The techniques we're describing today will proliferate across the threat landscape, which makes industry threat sharing, improved detection methods, and stronger safety controls all the more critical.

UTILITY DIVE

DIVE BRIEF

As cyber threats grow, utilities say lapsed information-sharing law stymies security

The Cybersecurity Information Sharing Act of 2015 has expired, and utilities say the U.S. faces a "more complex and dangerous security environment" as a result.

Published Oct. 20, 2025

Robert Walton
Senior Reporter

New threat groups are focused on operational technology and industrial control system environments where they can impact the delivery of services, Kristine Martz, a principal product advisor at cybersecurity firm Dragos, said Oct. 17, 2025 at a conference hosted by Columbia University's School of International and Public Affairs. Getty Images

Dive Brief:

- Amid rising threats to operational systems and a chaotic geopolitical environment, electric utilities want Congress to cleanly reauthorize the Cybersecurity Information Sharing Act of 2015, which allows for greater information sharing between the power sector and federal government.
- The law lapsed October 1. A temporary extension was included in the government funding bill, which failed and resulted in the current shutdown. A bipartisan Senate bill could bring CISA's protections back into force.
- It is vital that utilities are able to share threat information as the risks are rising, said Kristine Martz, a principal product advisor at cybersecurity firm Dragos. "Adversaries are becoming aware of the impact that they can achieve against easy to access

industrial control systems," or ICS, she said Friday at a conference hosted by Columbia University's School of International and Public Affairs.

Dive Insight:

"We've seen a consistent rise in threat activity over the years," Martz said**,** noting new threat adversaries are focused on operational technology and ICS environments where they can impact the delivery of services.

"They get in through these internet-facing devices and just live off the land for a long time to perform reconnaissance, pulling down things like your GIS data, your network maps," Martz said. "Living off the land" refers to cyber intruders using legitimate network tools to cover their presence and gain information.

While utility regulations like the North American Electric Reliability Corp.'s Critical Infrastructure Protection standards have helped create a baseline of security and shored up obvious weaknesses, Dragos has identified new threat groups developing operational and ICS-specific malware which take advantage of the extensive knowledge of utility work environments that hackers can gain from their research, Martz said.

Given the threat, and in an environment of rapidly growing electricity demand, it is vital that electric utilities are able to share information with government partners without fear of penalty, experts say.

The Edison Electric Institute, which represents investor-owned utilities, the Interstate Natural Gas Association of America, American Public Power Association, American Gas Association, National Electrical Manufacturers Association and the Electric Power Supply Association signed a letter in September urging a "clean" CISA 2015 reauthorization. The letter was led by

the U.S. Chamber of Commerce and included a wide range of organizations.

The law's lapse means the U.S. will face a "more complex and dangerous security environment," the groups said. CISA "provides safeguards for businesses regarding public disclosure, regulatory issues, and antitrust concerns to facilitate the timely exchange of information between the public and private sectors. Industry and government have a strong history of protecting privacy and civil liberties under this law," the groups said.

Reauthorizing the law will "ensure that businesses have legal certainty and protection against frivolous lawsuits when voluntarily sharing and receiving threat indicators and taking steps to mitigate cyberattacks," the groups said.

Congress failed to reauthorize the program despite broad support among Trump administration officials, lawmakers, industry leaders and cybersecurity experts. Senate Homeland Security Committee Chair Rand Paul, R-Ky., blocked efforts to save the program as he sought new restrictions on the law's efforts to combat online mis- and disinformation.

Bipartisan legislation introduced by Sens. Gary Peters, D-Mich., and Mike Rounds, R-S.D., would renew CISA for 10 years and would be retroactive to cover the lapse since the government shutdown began.

"Threat intelligence sharing between the private and public sector is vital in protecting critical infrastructure from cyberattacks," Dragos CEO Rob Lee said in a statement supporting the bill. "This critical cyber information sharing authority has given private entities the guardrails, and the confidence needed for responsible cooperation with the federal government. Those authorities must be renewed."

Kate Mabbett, director of security strategy and financial planning for American Electric Power, said during the Columbia panel that the reauthorization of CISA is a top security policy priority right now for the utility sector.

“I need to know I’m not going to be punished for sharing something that can better protect the nation,” Mabbett said.”There needs to be trust both ways — that I can share sensitive information about how I’m operating, and that the government is going to help protect that.”

ANNUAL THREAT ASSESSMENT

OF THE U.S. INTELLIGENCE COMMUNITY

Office of the Director of National Intelligence | March 2025

ANNUAL THREAT ASSESSMENT
OF THE U.S. INTELLIGENCE COMMUNITY

March 2025

INTRODUCTION

This annual report of worldwide threats to the national security of the United States responds to Section 617 of the FY21 *Intelligence Authorization Act* (Pub. L. No. 116-260). This report reflects the collective insights of the Intelligence Community (IC), which is committed to providing the nuanced, independent, and unvarnished intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world.

This assessment focuses on the most direct, serious threats to the United States primarily during the next year. All these threats require a robust intelligence response, including those where a near-term focus may help head off greater threats in the future.

Information available as of 18 March was used in the preparation of this assessment.

CONTENTS

FOREWORD

The 2025 Annual Threat Assessment (ATA) is the Intelligence Community's (IC) official, coordinated evaluation of an array of threats to U.S. citizens, the Homeland, and U.S. interests in the world. A diverse set of foreign actors are targeting U.S. health and safety, critical infrastructure, industries, wealth, and government. State adversaries and their proxies are also trying to weaken and displace U.S. economic and military power in their regions and across the globe.

Both state and nonstate actors pose multiple immediate threats to the Homeland and U.S. national interests. Terrorist and transnational criminal organizations are directly threatening our citizens. Cartels are largely responsible for the more than 52,000 U.S. deaths from synthetic opioids in the 12 months ending in October 2024 and helped facilitate the nearly three million illegal migrant arrivals in 2024, straining resources and putting U.S. communities at risk. A range of cyber and intelligence actors are targeting our wealth, critical infrastructure, telecom, and media. Nonstate groups are often enabled, both directly and indirectly, by state actors, such as China, as sources of precursors and equipment for drug traffickers. State adversaries have weapons that can strike U.S. territory, or disable vital U.S. systems in space, for coercive aims or actual war. These threats reinforce each other, creating a vastly more complex and dangerous security environment.

Russia, China, Iran and North Korea—individually and collectively—are challenging U.S. interests in the world by attacking or threatening others in their regions, with both asymmetric and conventional hard power tactics, and promoting alternative systems to compete with the United States, primarily in trade, finance, and security. They seek to challenge the United States and other countries through deliberate campaigns to gain an advantage, while also trying to avoid direct war. Growing cooperation between and among these adversaries is increasing their fortitude against the United States, the potential for hostilities with any one of them to draw in another, and pressure on other global actors to choose sides.

This 2025 ATA report supports the Office of the Director of National Intelligence's commitment to keeping the U.S. Congress and American people informed of threats to the nation's security, representing the IC's dedication to monitoring, evaluating, and warning of threats of all types. In preparing this assessment, the National Intelligence Council worked closely with all IC components, the wider U.S. Government, and foreign and external partners and experts to provide the most timely, objective, and useful insights for strategic warning and U.S. decision advantage.

This 2025 Annual Threat Assessment details these myriad threats by actor or perpetrator, starting with nonstate actors and then presenting threats posed by major state actors. The National Intelligence Council stands ready to support policymakers with additional information in a classified setting.

NONSTATE TRANSNATIONAL CRIMINALS AND TERRORISTS

Transnational criminals, terrorists, and other nonstate actors are threatening and impacting the lives of U.S. citizens, the security and prosperity of the Homeland, and U.S. strength at home and abroad. Some transnational criminal organizations (TCOs) are producing and trafficking large amounts of illicit drugs that are imperiling American lives and livelihoods. They are conducting other illegal activities that challenge U.S. security, such as human trafficking, cyber operations, money laundering, and inciting violence. U.S. citizens—at home and abroad—are also facing more diverse, complex, and decentralized terrorist threats. Actors, ranging from designated Foreign Terrorist Organizations—including the Islamic State of Iraq and ash-Sham (ISIS), al-Qa'ida, other Islamist terrorist groups, and some drug cartels— to terrorists acting alone or in small cells, are likely to pursue, enable, or inspire attacks. Finally, large-scale illegal immigration has strained local and national infrastructure and resources and enabled known or suspected terrorists to cross into the United States.

Foreign Illicit Drug Actors

Western Hemisphere-based TCOs and terrorists involved in illicit drug production and trafficking bound for the United States endanger the health and safety of millions of Americans and contribute to regional instability. Fentanyl and other synthetic opioids remain the most lethal drugs trafficked into the United States, causing more than 52,000 U.S. deaths in a 12-month period ending in October 2024. This represents a nearly 33 percent decrease in synthetic opioid-related overdose deaths compared to the same reporting time frame the previous year, according to CDC provisional data, and may be because of the availability and accessibility of naloxone.

- Mexico-based TCOs—including the Sinaloa Cartel and the New Generation Jalisco Cartel—remain the dominant producers and suppliers of illicit drugs, including fentanyl, heroin, methamphetamine, and South American-sourced cocaine, for the U.S. market. Last year, official points of entry along the U.S.-Mexico border were the main entry point for illicit drugs, often concealed in passenger vehicles and tractor trailers. However, some TCOs likely will at least temporarily change their smuggling techniques and routes in response to increased U.S. security force presence at the border.

- Since at least 2020, the growth of Mexico-based independent fentanyl producers—actors who are autonomous or semiautonomous from Mexican cartel control—has increasingly fragmented Mexico's fentanyl trade. Independent fentanyl producers are attracted to the drug's profitability and the low barriers to market entry, including the ease of synthesizing it using basic lab equipment and few personnel.

- Colombia-based TCOs and illegal armed groups are responsible for producing and exporting the vast majority of cocaine that reaches the United States, some of which is transshipped through Ecuador, contributing to an uptick in violent criminal conflicts that spurs regional migration.

- Mexico-based TCOs are ramping up lethal attacks in Mexico against rivals and Mexican security forces using IEDs, including landmines, mortars, and grenades. In 2024, there were nearly 1,600 attacks on Mexican security forces using IEDs, surging from only three reported attacks between 2020-2021. The sophistication of TCO tactics is reshaping Mexico's security landscape and has heightened the risk to security forces.

China remains the primary source country for illicit fentanyl precursor chemicals and pill pressing equipment, followed by India. Mexico-based chemical brokers circumvent international controls through mislabeled shipments and the purchase of unregulated dual-use chemicals.

Transnational Islamic Extremists

ISIS's most aggressive branches, including ISIS-Khorasan (ISIS-K), and its entrepreneurial plotters will continue to seek to attack the West, including the United States, via online outreach and propaganda aimed at directing, enabling, or inspiring attacks, and could exploit vulnerable travel routes. ISIS has suffered major setbacks and is incapable of holding ground in Iraq and Syria. In recent years, ISIS saw the U.S. defeat of its physical caliphate in 2019, the loss of three overall leaders in 2022, 2023, and 2025, and renewed counterterrorism efforts this year removing leaders driving global operations. Nevertheless, ISIS remains the world's largest Islamic terrorist organization, has sought to gain momentum from high-profile attacks, and continues to rely on its most capable branches and globally dispersed leadership to weather degradation.

The New Year's Day attacker in New Orleans was influenced by ISIS propaganda, and separately, an Afghan national was arrested in October for planning an election day attack in the name of ISIS, highlighting ISIS's ability to reach into the Homeland to both inspire and enable attacks.

- ISIS-K in South Asia is the group's branch most capable of carrying out external terrorist attacks and maintains the intent to conduct attacks in South and Central Asia, and globally, although its capabilities vary. ISIS-K's mass casualty attacks in Russia and Iran in 2024, as well as arrests of ISIS-K supporters in Europe and the United States, highlight the group's expanding capability beyond South Asia and ability to inspire individuals to conduct attacks abroad.

- ISIS will seek to exploit the end of the Asad regime in Syria to reconstitute its attack capabilities, including external plotting, and to free prisoners to rebuild their ranks.

- In 2024, the ISIS spokesman publicly hailed the group's Africa expansion, highlighting the growing importance of the continent to the group. ISIS-Somalia has doubled in size during the past year, ISIS-West Africa remains the largest branch and leads in numbers of claimed attacks, and ISIS-Sahel is expanding into coastal West Africa.

Al-Qa'ida maintains its intent to target the United States and U.S. citizens across its global affiliates. Its leaders, some of whom remain in Iran, have tried to exploit anti-Israeli sentiment over the war in Gaza to unite Muslims and encourage attacks against Israel and the United States. Al-Qa'ida's media apparatus issued statements from leaders and the group's affiliates supporting HAMAS and encouraging attacks against Israeli and U.S. targets.

- Al-Qa'ida in the Arabian Peninsula (AQAP) relaunched its *Inspire* guide with videos and tweets that encouraged attacks against Jewish targets, the United States, and Europe. *Inspire* provided instructions for making bombs and placing explosive devices on civilian airliners and gave religious, ideological, historical, and moral justification for such attacks. In addition to trying to inspire attacks worldwide and in the United States, AQAP has the intent to conduct operations in the region and beyond.

- Al-Shabaab—al-Qa'ida's largest and wealthiest affiliate—remains focused on attacks in Somalia that further its regional objectives, provides funding to al-Qa'ida efforts outside of Somalia, and has a

burgeoning relationship with the Huthis that could provide access to a new source of more sophisticated weapons, increasing the threat to U.S. interests in the region.

- In West Africa, al-Qa'ida is expanding its territorial control by gaining inroads with civilians through the provision of services and intimidation, and is threatening urban centers in Burkina Faso and Mali, where U.S. personnel are located.

- Al-Qa'ida's affiliate in Syria, Hurras al-Din, probably is exploiting the end of the Asad regime in Syria to strengthen its position. Despite its public announcement that the group was ordered dissolved by al-Qa'ida's senior leaders in Iran, Hurras al-Din members were advised not to disarm and instead to prepare for a future conflict, noting their continued fight against the Jews and their supporters.

Other Islamic terrorist groups—including some with historical ties to al-Qa'ida—continue to pose a threat to the United States primarily in the regions where they operate. Most of these groups generally have targeted local governments in recent years, while Lebanese Hizballah has continued to pursue limited targeting of primarily Israeli and Jewish individuals in and outside of the Middle East. The U.S. Government works with partners worldwide to prevent attacks against U.S. citizens, while watching for indications that these groups may shift intent and build capabilities to pursue transnational attacks.

- In South Asia, Tehrik-e-Taliban (TTP) operations in recent years have focused exclusively on targeting the Government of Pakistan, probably to avoid drawing more counterterrorism pressure. However, TTP's capabilities, historical ties to al-Qa'ida, and previous support to operations targeting the United States keep us concerned about the potential future threat. Anti-India groups, including Lashkar-e Tayyiba, similarly concern us in part because of their historical links with al-Qa'ida.

Other Transnational Criminals

Profit-motivated transnational criminals are using corruption, intimidation, and enabling technologies to expand their illegal activities into new markets and to diversify their sources of income, which increase their resiliency to U.S. and international law enforcement and financial regulatory efforts. TCOs are defrauding U.S. citizens, businesses, and government programs, while laundering billions of dollars of illicit proceeds through U.S. and international financial institutions. TCOs sometimes outsource money laundering operations and investments to individuals and networks with legal and banking expertise to circumvent financial regulations.

- TCOs and their financial facilitators use a myriad of methods to launder and repatriate illicit proceeds and to evade law enforcement and regulatory pressures. Some TCOs use digital currencies for money laundering and sanctions evasion activities because of its perceived anonymity and weaker international regulations compared to fiat currencies.

Financially motivated cyber criminals continue to prey on inadequately defended U.S. targets, such as healthcare systems and municipal governments, that could have broad impact on the U.S. populace and economy. Others have conducted attacks on critical infrastructure, disrupting utility company business networks or manipulating poorly secured control systems.

- Ransomware actors in mid-2024 attacked the largest payment processor for U.S. healthcare transactions, hampering prescriptions and causing extended delays in accessing electronic health records, patient communications, and medication ordering systems, and forcing some ambulances to divert patients to other hospitals.

- U.S. water infrastructure has become a more common target. In October 2024, criminal actors conducted cyber attacks against both large and small water utilities in the United States, possibly inspired by attacks against water infrastructure by Russian hacktivists and Iranian cyber actors in 2023 that had little effect but drew substantial publicity.

Foreign and U.S.-based human traffickers exploit vulnerable individuals and groups by promising well-paying jobs, confiscating identification documents, coercing victims to engage in risky behaviors and to work in inhumane conditions. TCOs that engage in human trafficking may also engage in other criminal activity threatening the United States, including fraud scams, drug trafficking, and weapons and human smuggling.

- Criminal actors, including Mexico-based TCOs, exploit migrants transiting the Western Hemisphere to the United States through kidnapping for ransom, forced labor, and sex trafficking operations. For example, some victims are forced to repay their smuggling fees through debt bondage once they arrive in the United States. These migrants are typically forced to become domestic servants, to work in the fishing, agriculture, and meat processing industries for low wages, or to work in illegal marijuana grow houses.

The total number of migrants trying to reach the United States has dropped significantly since January 2025 due to a surge in border security enforcement. While key drivers of migration in the Western Hemisphere, such as crime, poverty, and political repression, are likely to continue, heightened border security and mass deportation policies probably serve as a deterrent for migrants seeking to illegally cross U.S. borders.

- Law enforcement encounters with migrants at the U.S.-Mexico border were 14 percent lower in 2024 when compared to the previous year, and U.S. Border Patrol apprehensions along the Southwest border in January 2025 dropped 85 percent from the same period in 2024. Guatemalan, Mexican, and Venezuelan nationals were the most frequently encountered nationals at the U.S.-Mexico border.

- Real or perceived changes to immigration laws or travel polices in transit countries can trigger unexpected spikes. Since 2021, for instance, Nicaragua has removed visa requirements for air travelers from third countries, triggering a surge in U.S.-bound migration from those countries through Nicaragua.

MAJOR STATE ACTORS

Several major state actors present proximate and enduring threats to the United States and its interests in the world, challenging U.S. military and economic strength, regionally and globally. China stands out as the actor most capable of threatening U.S. interests globally, though it is also more cautious than Russia, Iran, and North Korea about risking its economic and diplomatic image in the world by being too aggressive and disruptive. Growing cooperation among these actors expands the threat, increasing the risk that should hostilities with one occur, it may draw in others.

CHINA

Strategic Overview

President Xi Jinping and the People's Republic of China (PRC) want to achieve "the great rejuvenation of the Chinese nation" by 2049. The PRC will seek to increase its power and influence to shape world events to create an environment favorable to PRC interests, obtain greater U.S. deference to China's interests, and fend off challenges to its reputation, legitimacy, and capabilities at home and abroad.

- Beijing is deeply suspicious of U.S. intentions and views Washington's measures against China as part of a concerted, whole-of-government effort, working with U.S. allies and partners, to contain China's development and rise, undermine CCP rule, and prevent the PRC from achieving its aims. PRC leaders are most concerned about strong unified opposition from the United States and its allies, and are responding, in part, by strengthening ties with partners like Russia and North Korea.

- At the same time, China's leaders will seek opportunities to reduce tension with Washington when they believe it benefits Beijing, protects its core interests, and buys time to strengthen its position.

The PRC will likely continue posturing to be in a position of advantage in a potential conflict with the United States. The PRC will continue trying to press Taiwan on unification and will continue conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage. China will likely struggle to sufficiently constrain the activities of PRC companies and criminal elements that enable the supply and trafficking of fentanyl precursors and synthetic opioids to the United States, absent greater law enforcement actions.

- China's military operations to project power over Taiwan and its efforts to assert sovereignty claims in the South and East China Seas occur routinely with confrontations that increase concern of miscalculations potentially leading to conflict.

- China has demonstrated the ability to compromise U.S. infrastructure through formidable cyber capabilities that it could employ during a conflict with the United States.

Beijing will continue to strengthen its conventional military capabilities and strategic forces, intensify competition in space, and sustain its industrial- and technology-intensive economic strategy to compete with U.S. economic power and global leadership.

Military

China presents the most comprehensive and robust military threat to U.S. national security. The People's Liberation Army (PLA) is fielding a joint force that is capable of full-spectrum warfare to challenge intervention by the United States in a regional contingency, projecting power globally, and securing what Beijing claims is its sovereign territory. A major portion of China's military modernization efforts is focused on developing counter-intervention capabilities tailored against all aspects of U.S. and allied military operations in the Pacific. Beijing will focus on meeting key modernization milestones by 2027 and 2035, aimed at making the PLA a world-class military by 2049.

- Examples of PLA advances in 2024 include the PLA Navy's third carrier (CV-18 Fujian) beginning sea trials and likely being ready to enter operational service in 2025. The PLA Rocket Force probably is fielding the DF-27 ballistic missile, with a hypersonic glide vehicle payload option and an estimated range of between 5,000 and 8,000 kilometers. The PLA ground forces are also fielding its most advanced multiple rocket launcher, the PCH191, increasing its long-range, precision strike capability.

- The PLA has improved its force structure, readiness, and training. The PLA probably has made particular progress in critical areas, such as modernizing key ground forces, expanding its navy with more modern combatants, and fielding a wide variety of new missile systems; it has also improved its electronic warfare (EW) capabilities.

The PLA has the capability to conduct long-range precision-strikes with conventional weapons against the Homeland's periphery in the Western Pacific, including Guam, Hawaii, and Alaska. China has developed a range of ballistic and cruise missiles with conventional payloads that can be delivered from its mainland as well as by air and sea, including by nuclear-powered submarines. China may be exploring development of conventionally-armed intercontinental range missile systems, which, if developed and fielded, would allow China to threaten conventional strikes against targets in the continental United States.

The PLA will continue to pursue the establishment of overseas military installations and access agreements to project power and protect China's interests abroad. Beijing may also pursue a mixture of military logistics models, including preferred access to commercial infrastructure abroad, exclusive PLA logistics facilities with pre-positioned supplies co-located with commercial infrastructure, and bases with stationed forces, to meet its overseas military logistics needs.

China is using complex, whole-of-government campaigns featuring coercive military, economic, and influence operations short of war to assert its positions and strength against others, reserving more destructive tools for full-scale conflict. Beijing will likely expand these campaigns to advance unification with Taiwan, project power in East Asia, and reverse perceived U.S. hegemony.

- Beijing has pushed back against U.S. military operations, such as reconnaissance and bomber flights, freedom of navigation operations, and exercises around PRC borders and maritime claims. The PLA regularly intercepts and shadows U.S. forces and sometimes conducts unsafe maneuvers in their vicinity.

Taiwan and Maritime Flashpoints

In 2025, Beijing will likely apply stronger coercive pressure against Taiwan and perceived increases in U.S. support to the island to further its goal of eventual unification. The PRC calls for a peaceful unification with Taiwan to resolve the Civil War that drove Taiwan's separation, even as it threatens to use force to compel unification if necessary and counter what it sees as a U.S. attempt to use Taiwan to undermine China's rise.

A conflict between China and Taiwan would disrupt U.S. access to trade and semiconductor technology critical to the global economy. Even without U.S. involvement in such a conflict, there would likely be significant and costly consequences to U.S. and global economic and security interests.

Beijing is working to isolate Taipei by pressuring states to downgrade diplomatic ties and support China's unification goal. Since 2016, Taiwan's official diplomatic relationships have dropped from 22 to only 12, and several of the remaining ones are vulnerable to Chinese pressure.

China is advancing military capabilities for a cross-Strait campaign while also using its armed forces to exert steady state pressure on Taiwan. The PLA probably is making steady but uneven progress on capabilities it would use in an attempt to seize Taiwan and deter—and if necessary, defeat—U.S. military intervention, and it is intensifying the scope, size, and pace of operations around Taiwan.

Beijing will continue to pressure Taipei with economic coercion and probably will increase it if it sees Taiwan taking steps toward formal independence. It could suspend preferential tariff terms, selectively ban Taiwan imports to China, and arbitrarily enforce regulations.

Beijing's aggressive efforts to assert sovereignty claims in the South and East China Seas are heightening tensions that could trigger a broader conflict.

- In 2024, PRC tactics in the South China Sea led to the loss of the Philippines' unilateral access to some disputed areas, and forced talks between Beijing and Manila in which the Philippines agreed to concessions in exchange for access. However, Manila is unlikely to relinquish its claims, creating potential for escalation by either side.
- Tension between China and Japan over the Senkaku Islands last flared up a decade ago. Since then, Chinese ships have remained in proximity of the disputed islands, occasionally entering the territorial zone, and driving responses from Japan's Self-Defense Force to monitor the activity.

Cyber

The PRC remains the most active and persistent cyber threat to U.S. government, private-sector, and critical infrastructure networks. The PRC's campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capabilities to compromise U.S. infrastructure.

- If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces.

Economics

The PRC seeks to compete with the United States as the leading economic power in the world. To do so, the strategy calls for a centralized, state-directed, and nationally resourced approach to dominating global markets and strategic supply chains, limiting foreign competitors, and making other nations dependent on China. PRC leaders are applying the same strategy to bolster China's position and become more globally dominant in critical supply chains, both in upstream inputs it can provide more cheaply than others and in downstream production at wider scale.

- China's weak domestic demand, coupled with its industrial policies, such as manufacturing subsidies, have enabled a surge in cheap Chinese exports in sectors such as steel, harming U.S. competitors and fueling a record PRC trade surplus.

- China's dominance in key supply chains enables its use of economic coercion against countries that adopt policies Beijing opposes. Beijing is developing an institutionalized framework enabling more assertive and centrally controlled trade retaliation. PRC leaders are using ostensibly unofficial or technical trade and investment barriers, administrative regulations, logistics, and symbolic sanctions in a targeted way against individuals, firms, and sectors, in parallel with messages to warn and deter.

- PRC leaders appear to be preparing for more economic friction with the United States, and probably are weighing options with the new U.S. administration while looking for leverage and other ways to prevent a major escalation and decoupling.

China's dominance in the mining and processing of several critical materials is a particular threat, providing it with the ability to restrict quantities and affect global prices. Beijing has shown a willingness to restrict global access to its mineral resources—sometimes in response to geopolitical disputes—as with its banning of exports to the United States of metals used in semiconductor manufacturing, such as gallium, germanium, and antimony in December 2024 in response to U.S. export controls on advanced semiconductors and chip-making equipment. Other examples include when the PRC temporarily stopped rare earth element exports to Japan in 2010, and Beijing's creation of new laws codifying its authority to restrict mineral exports. A prolonged cessation in supplies controlled by China could disrupt critical inputs needed for U.S. industry and technological advancements.

China has similar aims in global shipping and resource access, including in the Arctic, where melting sea ice is creating opportunities for expanded maritime transport and energy exploitation, especially along the Northern Sea Route (NSR) off Russia's coast. China seeks access to the Arctic's potentially vast natural resources, including oil, gas, and minerals, even though China is not among the eight Arctic countries that control territory in the region. Beijing seeks to normalize more direct and efficient maritime shipping routes to Russia and other Northern Hemisphere areas, as a way to fuel its economic growth and energy security and reduce its dependence on Middle East energy. China has gradually increased engagement with Greenland mainly through mining projects, infrastructure development, and scientific research projects. Despite less active engagement right now, China's long-term goal is to expand access to Greenland's natural resources, as well as to use the same access as a key strategic foothold for advancing China's broader and economic aims in the Arctic.

Technology

China is using an aggressive, whole-of-government approach, combined with state direction of the private sector, to become a global S&T superpower, surpass the United States, promote self-reliance, and achieve further economic, political, and military gain. Beijing has prioritized technology sectors such as advanced power and energy, AI, biotechnology, quantum information science, and semiconductors, further challenging U.S. efforts to protect critical technologies by tailoring restrictions narrowly to address national security concerns. China is accelerating its S&T progress through a range of licit and illicit means, to include investments, intellectual property acquisition and theft, cyber operations, talent recruitment, international collaborations, and sanctions evasion.

- Some forecasts indicate China's technology sectors will account for as much as 23 percent of its gross domestic product by 2026, more than doubling since 2018. In addition to private funding, the PRC government is investing hundreds of billions of dollars in priority technologies, such as AI, microelectronics, and biotechnologies, in pursuit of its self-reliance goals.

China almost certainly has a multifaceted, national-level strategy designed to displace the United States as the world's most influential AI power by 2030. China is experiencing a boom in generative AI with the rapid emergence of a large number of PRC-developed models, and is broadly pursuing AI for smart cities, mass surveillance, healthcare, S&T innovation, and intelligent weapons. Chinese AI firms are already world leaders in voice and image recognition, video analytics, and mass surveillance technologies. The PLA probably plans to use large language models (LLMs) to generate information deception attacks, create fake news, imitate personas, and enable attack networks. China has also announced initiatives to bolster international support for its vision of AI governance.

- China has stolen hundreds of gigabytes of intellectual property from companies in Asia, Europe, and North America in an effort to leapfrog over technological hurdles, with as much as 80 percent of U.S. economic espionage cases as of 2021 involving PRC entities.

China also sees biotechnology as critical to becoming a dominant economic power and intends to grow its domestic bioeconomy to $3.3 trillion this year. Beijing is investing heavily in collecting health and genetic data both at home and abroad in pursuit of these goals, and has shown it can be globally competitive in certain low-cost, high-volume commodities, such as biomanufacturing and genetic sequencing. Beijing has identified genetic data as a national strategic resource and is expanding state control over the country's gene banks and other genetic repositories, positioning it to potentially lead in precision medicine and agricultural biotechnology applications.

China has made progress in producing advanced 7-nanometer (nm) semiconductor chips for cryptocurrency mining and cellular devices using previously acquired deep ultraviolet (DUV) lithography equipment, but will face challenges achieving high-quality, high-volume production of these chips without access to extreme ultraviolet lithography tools. PRC researchers also continue to explore applying advanced patterning techniques to DUV machines to produce semiconductor chips as small as 3nm. China leads the world in legacy logic semiconductor (28nm and up) production, accounting for 39.3 percent of global capacity, and is expected to add more capacity than the rest of the world combined through 2028. These legacy chips are vital to producing automobiles, consumer electronics, home appliances, factory automation, broadband, and many military and medical systems.

WMD

China remains intent on modernizing, diversifying, and expanding its nuclear posture. China's nuclear weapons and advanced delivery systems pose a direct threat to the Homeland and are capable of delivering catastrophic damage to the United States and threatening U.S. military forces here and abroad.

China most likely possesses capabilities relevant to chemical and biological warfare (CBW) that pose a threat to U.S., allied, and partner forces as well as civilian populations.

Biosecurity

China's approach to and role in global biological, medical, and other health-related global priorities present unique challenges to the United States and the world The COVID-19 pandemic that ultimately led to the death of more than one million Americans—and multiples more worldwide—began in China, which Beijing still refuses to acknowledge. China's strict censorship and repression of free speech prevented doctors treating the earliest of patients in Wuhan from warning the world of a far more serious contagion than Beijing wanted told, slowing the world's preparedness and response. To this day, Beijing refuses to fully cooperate with the rest of the international community trying to definitively pinpoint the precise cause of the disease so it can head off and prepare for any new disease.

Regarding COVID-19 origins, IC agencies have continued to evaluate new information from classified and open sources, revisit previous reporting, and consult with diverse technical experts to increase our understanding of the cause of the pandemic. These efforts have led CIA to assess that a research-related hypothesis is more likely than a natural origin hypothesis.

The other hypothesis for COVID-19—natural origin—includes many scenarios in which humans could have been infected with SARS-CoV-2—the virus that causes COVID-19—or a close progenitor through exposure to wild or domestic animals. China is home to a diverse body of naturally occurring coronaviruses found in a wide geographic area, and there is precedence for these viruses to emerge within human populations far from reservoir locations. For example, the coronavirus that is the closest known relative to SARS-CoV—the virus that causes severe acute respiratory syndrome (SARS)—probably originated in Yunnan Province, according to scientific studies, even though the first SARS outbreak detected in humans in 2003 occurred in Guangdong Province, hundreds of miles away.

- The research-related incident hypothesis also considers a broad range of potential initial human-infection scenarios from events in research facilities, such as government or university laboratories, to research-related activities in the field, such as collecting samples from wild animals.

The PRC's dominance in pharmaceutical and medical supply production combined with lower quality safety and environmental standards than those of the United States positions Beijing to potentially restrict such exports for leverage over Washington and others in trade or security disputes. The PRC plays an increasingly important role in supplying pharmaceuticals and related medical supplies to the United States, as well as the rest of the world.

- U.S. imports of Chinese pharmaceuticals—defined as medicines, vaccines, blood, organic cultures, bandages, and organs—grew almost five-fold between 2020 and 2022 alone, from $2.1 billion to $10.3 billion.

- The PRC also might look to uniquely provide such supplies and medical aid to countries, more cheaply and at scales competitors cannot match, as a way to boost its global influence at the expense of the United States. The PRC's "vaccine diplomacy" during the COVID-19 pandemic—it provided vaccines to 83 countries—was driven at least in part by geopolitical considerations, such as currying favor for a new port in Burma.

Space

China has eclipsed Russia as a space leader and is poised to compete with the United States as the world's leader in space by deploying increasingly capable interconnected multi-sensor systems and working toward ambitious scientific and strategic goals. China has achieved global coverage in some of its intelligence, surveillance, and reconnaissance (ISR) constellations and world-class status in all but a few space technologies.

- China's Beidou constellation is a world-class position, navigation, and timing capability that competes with U.S. GPS and Europe's Galileo service. The PLA ISR architecture and satellite communications are areas the PLA continues to improve upon to close the perceived gap between itself and the U.S. military.

- China's successful lunar sample return mission in June 2024 contributes to Beijing's technological prowess and national prestige while supporting its effort to land astronauts on the Moon by 2030 and establish the first lunar base by 2035.

- China's commercial space sector is growing quickly with aspiration to be a major global competitor to U.S. and European space companies. For example, China launched the first set of satellites in its low Earth orbit (LEO) proliferated constellation last year for its own satellite Internet service to compete with Western commercial satellite Internet services.

Counterspace operations will be integral to PLA military campaigns, and China has counterspace-weapons capabilities intended to target U.S. and allied satellites. China already has fielded ground-based counterspace capabilities, including EW systems, directed energy weapons (DEWs), and antisatellite (ASAT) missiles intended to disrupt, damage, and destroy target satellites.

- China also has conducted orbital technology demonstrations, which, while not counterspace weapons tests, prove its ability to operate future space-based counterspace weapons. China has also conducted on-orbit satellite inspections of other satellites, which probably would be representative of the tactics required for some counterspace attacks.

Malign Influence Activities

Beijing will continue to expand its coercive and subversive malign influence activities to weaken the United States internally and globally, as well as counter what Beijing sees as a U.S.-led campaign to tarnish China's global relations and overthrow the CCP. Through these efforts, the PRC seeks to suppress critical views and critics of China within the United States and worldwide, and sow doubts in U.S. leadership and strength. Beijing is likely to feel emboldened to use malign influence more regularly in coming years, particularly as it fields AI to improve its capabilities and avoid detection.

- PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation. For example, pro-China online actors in 2024 used AI-generated news anchors and fake social media accounts with AI-generated profile pictures to sow divisions on issues such as drug use, immigration, and abortion.

China's Challenges

China faces daunting challenges that will impair CCP leaders' strategic and political achievements. China's leaders probably are most concerned about corruption, demographic imbalances, and fiscal and economic struggles because they threaten the country's economic performance and quality of life, two key factors underpinning CCP legitimacy. Despite an acute economic slowdown, China's leaders probably will resist making needed structural reforms and instead maintain statist economic policies to steer capital toward priority sectors, reduce dependence on foreign technologies, and enable military modernization.

- China's growth probably will continue to slow because of low consumer and investor confidence. China's birth and marriage rates continue to decline, reinforcing negative population trends and a shrinking labor force.

Xi's focus on security and stability for the CCP and securing other leaders' personal loyalty to him is undermining China's ability to solve complex domestic problems and will impede Beijing's global leverage. Xi's blending of domestic and foreign security threats is undermining China's position and standing abroad, reducing Beijing's ability to shape global perceptions and compete with U.S. leadership.

RUSSIA

Strategic Overview

Russia views its ongoing war in Ukraine as a proxy conflict with the West, and its objective to restore Russian strength and security in its near abroad against perceived U.S. and Western encroachment has increased the risks of unintended escalation between Russia and NATO. The resulting heightened and prolonged political-military tensions between Moscow and Washington, coupled with Russia's growing confidence in its battlefield superiority and defense industrial base and increased risk of nuclear war, create both urgency and complications for U.S. efforts to bring the war to an acceptable close.

Regardless of how and when the war in Ukraine ends, Russia's current geopolitical, economic, military, and domestic political trends underscore its resilience and enduring potential threat to U.S. power, presence, and global interests. Despite having paid enormous military and economic costs in its war with Ukraine, Russia has proven adaptable and resilient, in part because of the expanded backing of China, Iran, and North Korea. President Vladimir Putin appears resolved and prepared to pay a very high price to prevail in what he sees as a defining time in Russia's strategic competition with the United States, world history, and his personal legacy. Most Russian people continue to passively accept the war, and the emergence of an alternative to Putin probably is less likely now than at any point in his quarter-century rule.

- Western efforts to isolate and sanction Russia have accelerated its investments in alternative partnerships and use of various tools of statecraft to offset U.S. power, with China's backing and reinforcement. Russia's relationship with China has helped Moscow circumvent sanctions and export controls to continue the war effort, maintain a strong market for energy products, and promote a global counterweight to the United States, even if at the cost of greater vulnerability to Chinese influence. Russia is also increasing military cooperation with Iran and North Korea, which will continue to help its war effort and enhance U.S. adversary cooperation and collective capacity. Finally, Moscow is increasingly willing to play spoiler in Western-centric forums such as the UN as well as use non-Western organizations like the Brazil, Russia, India, China, and South Africa (BRICS) group to press policies such as de-dollarization.

- Russia has shown it can navigate substantial economic challenges resulting from the ongoing drains of the war, Western cost imposition, and high inflation and interest rates, for at least the near term by using financial and import substitution workarounds, maintaining low debt, and continuing investments in the defense-industrial base. Russia's economy remains the fourth largest in the world (based on GDP at purchasing power parity).

- Russia's sizable ground force losses in the war have done little to undermine the strategic pillars of its military power, to include its diverse and robust nuclear deterrent and asymmetric capabilities, particularly in counterspace and undersea warfare. Russia's air and naval forces remain intact, with the former being more modern and capable than at the start of the invasion. Russia is developing a growing arsenal of conventional capabilities, such as theater strike weapons, to target the Homeland and deployed forces and assets abroad—and to hold U.S. allies at risk—during crisis and wartime. Russia's advanced WMD and space programs threaten the Homeland, U.S. forces, and key warfighting advantages.

- Russia will continue to be able to deploy anti-U.S. diplomacy, coercive energy tactics, disinformation, espionage, influence operations, military intimidation, cyberattacks, and gray zone tools to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests.

- The war in Ukraine has afforded Moscow a wealth of lessons regarding combat against Western weapons and intelligence in a large-scale war. This experience probably will challenge future U.S. defense planning, including against other adversaries with whom Moscow is sharing those lessons learned.

Russia and the Arctic

Russia controls about half of all Arctic coastline and views the region as essential to its economic well-being and national security. Moscow wants to further develop its Arctic oil and gas reserves and position itself to reap benefits from expected increases in maritime trade. Russia has concerns about increasing economic and military competition with Western countries in the region, which compounded last year when NATO enlarged to include the last two previously nonaligned Arctic states, Finland and Sweden.

- The war in Ukraine has sapped Russia's finances and available military resources to fulfill its Arctic ambitions, prompting Russia to seek a closer partnership with China in the Arctic, and

welcoming other non-Western countries' increasing involvement, to offset NATO countries' perceived advantages.

- Russia's interest in Greenland is focused mainly on its proximity to strategically important naval routes between the Arctic and Atlantic Oceans—including for nuclear-armed submarines—and the fact that Greenland hosts a key U.S. military base.

Military

Moscow's massive investments in its defense sector will render the Russian military a continued threat to U.S. national security, despite Russia's significant personnel and equipment losses—primarily in the ground forces—during the war with Ukraine. Russia's air and naval forces, despite suffering some losses and expending substantial quantities of precision-guided munitions, remain capable of providing Moscow with regional and global power projection forces, while Russia's nuclear and counterspace forces continue to provide it with strategic deterrence capability.

- The Ukraine conflict has led to improvements in some Russian military capabilities. For example, Russia's initial use of EW and unmanned systems was lacking but it adapted and innovated using EW to more effectively interfere with Ukrainian use of radar and GPS and unmanned aerial vehicles (UAVs).

- Russia possesses long-range precision strike capability, most notably submarines and bombers equipped with LACMs and antiship cruise missiles, that can hold the Homeland at risk.

- Moscow has increased its defense budget to its heaviest burden level during Putin's more than two decades in power and taken measures to reduce the impact of sanctions on its military and defense industry.

- Russia has imported munitions such as UAVs from Iran and artillery shells from North Korea to mitigate to the impact of international sanctions, thereby sustaining its ability to wage war in Ukraine and enhancing the threat its military poses.

Moscow will contend with long-term challenges such as troop quality and corruption, and a fertility rate below what is needed for replacements, but its investments in personnel recruitment and procurement should allow it to steadily reconstitute reserves and expand ground forces in particular during the next decade. Nevertheless, the war in Ukraine will be a drag on those efforts as long as it persists. Moscow will have to continually balance resource allocation between large-scale production of equipment to sustain the war with modernization and recapitalization efforts.

Russia and Ukraine

Russia in the past year has seized the upper hand in its full-scale invasion of Ukraine and is on a path to accrue greater leverage to press Kyiv and its Western backers to negotiate an end to the war that grants Moscow concessions it seeks. Continuing the Russia-Ukraine war perpetuates strategic risks to the United States of unintended escalation to large-scale war, the potential use of nuclear weapons, heightened insecurity among NATO Allies, particularly in Central, Eastern, and Northern Europe, and a more emboldened China and North Korea.

Even though Russian President Putin will be unable to achieve the total victory he envisioned when initiating the large-scale invasion in February 2022, Russia retains momentum as a grinding war of attrition plays to Russia's military advantages. This grinding war of attrition will lead to a gradual but steady erosion of Kyiv's position on the battlefield, regardless of any U.S. or allied attempts to impose new and greater costs on Moscow.

- Despite recruitment challenges, Russia has regularly generated sufficient personnel to replenish losses and create new units to sustain attacks on multiple frontline axes. While Ukraine has increased its overall personnel intake since new legislation on mobilization was passed in spring 2024, Kyiv has stretched its resources trying to launch new offensives—such as in Kursk, Russia—and build more brigades while defending on all fronts.

- Moscow's rising defense spending and investments in defense-industrial capacity will continue to enable a high level of production of critical capabilities—such as artillery, long-range missiles, one-way attack UAVs, and glide bombs—and ensure Russia retains a firepower advantage over Ukraine.

- Both Putin and Ukrainian President Volodymyr Zelenskyy are interested in continuing discussions with the United States on how to end the war and have shown a willingness to test partial ceasefires. Nonetheless, Putin probably is attuned to the potential for protracted conflict to drag down the Russian economy and prompt undesired escalation with the West, and Zelenskyy probably understands that his position is weakening, the future of Western assistance is uncertain, and a ceasefire may ultimately become a necessary recourse. However, both leaders for now probably still see the risks of a longer war as less than those of an unsatisfying settlement. For Russia, positive battlefield trends allow for some strategic patience, and for Ukraine, conceding territory or neutrality to Russia without substantial security guarantees from the West could prompt domestic backlash and future insecurity.

Cyber

Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat. Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict.

- Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware.

Malign Influence Activities

Moscow uses influence activities to counter threats, including by stoking political discord in the West, sowing doubt in democratic processes and U.S. global leadership, degrading Western support for Ukraine, and amplifying preferred Russian narratives. Moscow's malign influence activities will continue for the foreseeable future and will almost certainly increase in sophistication and volume.

- Moscow probably believes information operations efforts to influence U.S. elections are advantageous, regardless of whether they affect election outcomes, because reinforcing doubt in the integrity of the U.S. electoral system achieves one of its core objectives.

- Russia uses a variety of entities such as the U.S.-sanctioned influence organizations Social Design Agency (SDA) and ANO Dialog and the state media outlet RT in its efforts to covertly shape public opinion in the United States, amplify and stoke domestic divisions, and discreetly engage Americans, while hiding Russia's hand.

WMD

Russia has the largest and most diverse nuclear weapons stockpile that, along with its deployed ground-, air-, and sea-based delivery systems, could inflict catastrophic damage to the Homeland. Russia has developed a more modernized, mobile, and survivable strategic nuclear force that is intended to circumvent or neutralize future augmented U.S. missile defense and ensure deterrence through reliable retaliatory strike potential. In addition, Russia's vast arsenal of non-strategic nuclear weapons helps it to offset Western conventional superiority and provide formidable escalation management options in theater war scenarios.

Russia continues efforts to modernize its nuclear weapons capabilities in the face of multiple failed tests of new systems.

Russia's CBW threat is expanding. Russian scientific institutes continue to research and develop CBW capabilities, including technologies to deliver CBW agents. Russia retains an undeclared chemical weapons program and has used chemical weapons at least twice during recent years in assassination attempts with Novichok nerve agents, also known as fourth-generation agents, against Russian opposition leader Aleksey Navalny in 2020, and against U.K. citizen Sergey Skripal and his daughter Yuliya Skripal on U.K. soil in 2018. Russian forces almost certainly continue using chemicals against Ukrainian forces, with hundreds of reported attacks occurring since late 2022.

Space

Russia continues to train its military space elements and field new antisatellite weapons to disrupt and degrade U.S. and allied space capabilities. It is expanding its arsenal of jamming systems, DEWs, on-orbit counterspace capabilities, and ASAT missiles designed to target U.S. and allied satellites.

- Russia is using EW to counter Western on-orbit assets and continues to develop ASAT missiles capable of destroying space targets in LEO.

Despite its Soviet legacy, the war in Ukraine has revealed glaring deficiencies in Russia's space-based architecture, which will continue to face difficulties from the effects of sanctions and export controls, domestic space-sector problems, and increasingly strained competition for program resources within Russia. However, Russia will remain a space competitor, probably by prioritizing assets critical to its national security and integrating military space services over civil space projects.

- Moscow uses its and others' civil and commercial remote-sensing satellites to supplement military-dedicated capabilities and has warned that other countries' commercial infrastructure in outer space used for military purposes can become a legitimate target.

Russian Antisatellite Capability

Russia is developing a new satellite meant to carry a nuclear weapon as an antisatellite capability. A nuclear detonation in outer space could cause devastating consequences for the United States, the global economy, and the world in general. It would harm all countries' national security and commercial satellites and infrastructure, as well as impair U.S. use of space as a driver for economic development.

- In February 2022, Russia launched a satellite, which its Ministry of Defense claimed at the time was for testing on-board instruments and systems under the influence of radiation and heavy charged particles.

Technology

While Russia's S&T ecosystem has been constrained in the wake of its invasion of Ukraine, Moscow continues to deploy nascent AI applications on and off the battlefield and has deepened technical cooperation with partners such as China in support of long-term R&D goals. Moscow's use of AI to augment military operations probably will further hone Russian tactics and capabilities in the event of future conflicts with the United States or NATO allies.

- Russia is using AI to create highly-capable deepfakes to spread misinformation, conduct malign influence operations, and stoke further fear. Russia has also demonstrated the use of AI-enabled antidrone equipment during its ongoing conflict with Ukraine.

- Russia's few domestic microelectronics manufacturers have only mastered production of chips down to the 65nm level and has goals of mass producing 28nm chips by 2030, significantly behind global leaders.

- While largely cut-off from Western supply chains, Russia has significantly expanded and deepened cooperation in several technical sectors with international partners. Russia seeks to further align its S&T efforts with China and BRICS allies in areas such as AI development and governance and semiconductor production to advance its own capabilities as well as broadly decrease Western influence.

Russia's Challenges

Even as Russia has proven resilient, it faces a myriad of challenges to remaining an indispensable global player, maintaining a sphere of influence, and upholding stability at home—its highest strategic aims—suggesting limits on its confidence dealing with the United States and the international community. Russia has paid a heavy price in blood, treasure, and loss of international reputation and foreign policy options because of its large-scale invasion of Ukraine. President Putin upended two decades of Russia's geopolitical resurgence, created new threats to its external and internal security, and strained its economic and military potential, making it more reliant on China and other like-minded partners like North Korea.

- Russia's military has suffered more casualties in Ukraine than in all of its other wars since World War II (750,000-plus dead and wounded), and its economy faces significant long-term macroeconomic headwinds and is increasingly dependent on China.
- Russia's aggression has strengthened European unity and prompted Finland and Sweden to join NATO. Efforts by Armenia, Moldova, and some Central Asian states to seek alternative partners highlight how the war has hurt Moscow's influence, even in the post-Soviet space, and derailed Putin's vision of a greater Eurasian union.

IRAN

Strategic Overview

Tehran will try to leverage its robust missile capability and expanded nuclear program, and its diplomatic outreach to regional states and U.S. rivals to bolster its regional influence and ensure regime survival. However, regional and domestic challenges, most immediately tensions with Israel, are seriously testing Iran's ambitions and capabilities. A degraded Hizballah, the demise of the Asad regime in Syria, and Iran's own failure to deter Israel have led leaders in Tehran to raise fundamental questions regarding Iran's approach. Iran's consistently underperforming economy and societal grievances will also continue to test the regime domestically.

Tehran will continue its efforts to counter Israel and press the United States to leave the region by aiding and arming its loose consortium of like-minded terrorist and militant actors, known as the "Axis of Resistance." Although the demise of the Asad regime, a key ally of Tehran, is a blow to the Axis, these actors still represent a wide range of threats. These threats include some continued Israeli vulnerability to HAMAS and Hizballah; militia attacks against U.S. forces in Iraq and Syria; and the threat of Huthi missile and UAV attacks targeting Israel and maritime traffic transiting near Yemen. Supreme Leader Ali Khamenei continues to desire to avoid embroiling Iran in an expanded, direct conflict with the United States and its allies.

Iranian investment in its military has been a key plank of its efforts to confront diverse threats and try to deter and defend against an attack by the United States or Israel. Iran continues to bolster the lethality and precision of its domestically produced missile and UAV systems, and it has the largest stockpiles of these systems in the region. It considers them as critical to its deterrence strategy and power projection capability, and Iran uses their sales to deepen global military partnerships. Iran's growing expertise and willingness to conduct aggressive cyber operations also make it a major threat to the security of U.S. and allied and partner networks and data.

Iran also will continue to directly threaten U.S. persons globally and remains committed to its decade-long effort to develop surrogate networks inside the United States. Iran seeks to target former and current U.S. officials it believes were involved in the killing of Islamic Revolutionary Guard Corps (IRGC)-Qods Force Commander Qasem Soleimani in January 2020 and previously has tried to conduct lethal operations in the United States.

Tehran intends for its expanding relationships with other key U.S. adversaries and the Global South to mitigate U.S. efforts to isolate the regime and blunt the impact of Western sanctions. Tehran's diplomatic efforts—including at times outreach to Europe—are likely to continue with varying degrees of success. In the past year, Iran has focused extensively on deepening ties with Russia—including through military cooperation for its war in Ukraine—and has relied on China as a key political and economic partner to help it mitigate economic and diplomatic pressure. Iran is also making progress developing closer diplomatic and defense ties to African states and other actors in the Global South and is trying to build on nascent improvements in its ties with other regional actors, such as Saudi Arabia, despite continued mutual suspicion over each other's ultimate visions for the region.

The economic, political, and societal seeds of popular discontent could threaten further domestic strife akin to the widescale and prolonged protests inside Iran during late 2022 and early 2023. The economy is beset by low growth, exchange rate volatility, and high inflation. Absent sanctions relief, these trends probably will continue for the foreseeable future.

Syria

The fall of President Bashar al-Asad's regime at the hands of opposition forces led by Hay'at Tahrir al-Sham (HTS)—a group formerly associated with al-Qa'ida—has created conditions for extended instability in Syria and could contribute to a resurgence of ISIS and other Islamist terror groups. Even if the HTS–led interim government can bridge divergent objectives, governing Syria will remain a daunting challenge amid the country's economic problems, humanitarian needs driven in part by millions of internally displaced Syrians, rampant insecurity, as well as ethnic, sectarian, and religious cleavages.

- The HTS-led interim government forces, along with elements of Hurras al-Din and other jihadist groups, engaged in violence and extrajudicial killings in northwestern Syria in early March 2025 primarily targeting religious minorities that resulted in the death of more than 1,000 people, including Alawi and Christian civilians.
- The leader of HTS claims to be willing to work with Syria's array of ethnosectarian groups to develop an inclusive governance model. Many of these groups remain skeptical of HTS's intentions, especially considering the leader's past al-Qa'ida association, suggesting protracted negotiations could devolve into violence. Israeli government officials are skeptical of HTS claims and intentions, expressing concern that historical HTS objectives against Israel persist.
- Some remaining jihadist groups refuse to merge into the HTS Ministry of Defense, and ISIS has already signaled opposition to HTS's call for democracy and is plotting attacks to undermine its governance.

Military

Iran's conventional and unconventional capabilities will pose a threat to U.S. forces and partners in the region for the foreseeable future, despite the degradation to its proxies and air defenses during the Gaza conflict. Iran's large conventional forces are capable of inflicting substantial damage to an attacker, executing regional strikes, and disrupting shipping, particularly energy supplies, through the Strait of Hormuz. Iran's unconventional warfare operations and militant partners and proxies, such as Hizballah, have traditionally enabled Tehran to pursue its interests throughout the region and maintain strategic depth with a modicum of deniability. However, Iranian officials are grappling with how to slow and eventually reverse their and their proxies' recent military losses from the Israeli campaign against Iran and its regional allies, including strikes on Iranian military targets such as air defense systems in April and October 2024. The IC assesses Iran's prospects for reconstituting force losses and posing a credible deterrent, particularly to Israeli actions, are dim in the near-term.

Iran has fielded a large quantity of ballistic and cruise missiles as well as UAVs that can strike throughout the region and continues efforts to improve their accuracy, lethality, and reliability. Iran's defense industry has a robust development and manufacturing capacity, especially for low-cost weapons such as small UAVs. However, the limited damage Iran's strikes in April and October 2024 inflicted on Israel highlights the shortcomings of Iran's conventional military options.

Iran has also deployed small boats and submarines capable of disrupting shipping traffic through the Strait of Hormuz. Its ground and air forces, while among the largest in the region, suffer from outdated equipment and limited training.

Middle East Conflict

The Israel-HAMAS conflict sparked by the HAMAS October 7 attack against Israel derailed the unprecedented diplomacy and cooperation generated by the Abraham Accords and trajectory of growing stability in the Middle East. We expect the situation in Gaza, as well as Israel-Hizballah and Israel–Iran dynamics, to remain volatile.

Even in degraded form, HAMAS continues to pose a threat to Israeli security. The group retains thousands of fighters and much of its underground infrastructure, and probably has used the ceasefire to reinforce and resupply its military and munitions stock so that it can fight again. HAMAS is capable of resuming a low-level guerilla resistance and to remain the dominant political action in Gaza for the foreseeable future. Low expectations on all sides that a ceasefire will endure and the absence of a credible post-fighting political and reconstruction plan, portend years of instability.

- While HAMAS's popularity has declined among Gazans, its popularity remains high among West Bank Palestinians, especially relative to the Palestinian Authority (PA).

The long-term Israeli-Palestinian relationship also hinges on the trajectory of an increasingly unstable West Bank. The PA's weak and declining ability to provide security and other services in the West Bank, Israeli operations in the West Bank, violence from Israeli settlers and Palestinian militant groups including HAMAS, and a potential leadership transition in the PA are likely to exacerbate governance challenges in Ramallah. Much also will depend on how Israel deals with post-conflict Gaza and its operations in the West Bank that may weaken or undermine the PA.

During the Gaza conflict, Iran encouraged and enabled its various proxies and partners to conduct strikes against Israeli and at times U.S. forces and interests in the region.

- The Huthis have emerged as the most aggressive actor, attacking commercial shipping in the Red Sea and Indian Ocean, U.S. and European forces, and Israel. In addition to receiving Iranian assistance, the Huthis have expanded their reach by broadening partnerships with other actors, such as Russia and Russian arms brokers, PRC commercial defense companies, al-Shabaab, and Iraqi Shia militants.

- Iraqi Shia militias continue to try to compel a U.S. withdrawal from Iraq through political pressure on the Iraqi government and attacks on U.S. forces in Iraq and Syria.

Further fighting between Hizballah and Israel would threaten Lebanon's fragile stability and any political progress begun by the election of a president in January after years of trying. A resumption of protracted Israeli operations in Lebanon could trigger a sharp rise in sectarian tension, undermine Lebanese security forces, and dramatically worsen humanitarian conditions. Although weakened, Hizballah maintains the capability to target U.S. persons and interests in the region, worldwide, and—to a lesser extent—in the United States.

Cyber

Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. networks and data. Guidance from Iranian leaders has incentivized cyber actors to become more aggressive in developing capabilities to conduct cyber attacks.

Malign Influence Activities

Iran often amplifies its influence operations with offensive cyber activities. During the Israel-HAMAS conflict, U.S. private industry tracked Iranian influence campaigns and cyber attacks.

- In June 2024, an IRGC actor compromised an email account associated with an individual with informal ties to then-former President Trump's campaign and used that account to send a targeted spear-phishing email to individuals inside the campaign itself. The IRGC subsequently tried to manipulate U.S. journalists into leaking information illicitly acquired from the campaign.

WMD

We continue to assess Iran is not building a nuclear weapon and that Khamenei has not reauthorized the nuclear weapons program he suspended in 2003, though pressure has probably built on him to do so. In the past year, there has been an erosion of a decades-long taboo on discussing nuclear weapons in public that has emboldened nuclear weapons advocates within Iran's decisionmaking apparatus. Khamenei remains the final decisionmaker over Iran's nuclear program, to include any decision to develop nuclear weapons.

Iran very likely aims to continue R&D of chemical and biological agents for offensive purposes. Iranian military scientists have researched chemicals that have a wide range of sedation, dissociation, and amnestic incapacitating effects, and can also be lethal.

Iran's Challenges

Iranian leaders recognize the country is at one of its most fragile points since the Iran-Iraq war, which probably weighs on their strategic calculus and confidence in their approach toward the region, the United States, and U.S. partners. They face growing political, social, economic, and regional pressures, leaving Iran increasingly vulnerable to regime-threatening instability and external interference.

NORTH KOREA

Strategic Overview

North Korean leader Kim Jong Un will continue to pursue strategic and conventional military capabilities that target the Homeland, threaten U.S. and allied armed forces and citizens, and enable Kim to undermine U.S. power and reshape the regional security environment in his favor. Kim's newly cemented strategic partnership with Russia is yielding financial benefit, diplomatic support, and defense cooperation. The partnership with

Moscow also helps reduce Pyongyang's reliance on Beijing. North Korea's advancing strategic weapons capabilities and increasing access to revenue are enabling Kim's longstanding goals of securing international acceptance as a nuclear power, reducing U.S. military presence on the Korean Peninsula, expanding state control over the North's economy, and blocking foreign influence.

- In June 2024, Kim and Putin signed a comprehensive strategic agreement for sweeping economic and technology partnerships. Kim also is using the agreement's mutual defense clause, which commits each country to provide military assistance if either is invaded by a foreign power, to justify deploying combat troops to fight against Ukraine.

- Kim has no intention of negotiating away his strategic weapons programs, which he perceives as a guarantor of regime security and national pride, because they threaten the Homeland, U.S. forces in the region, and U.S. allies like South Korea and Japan. He is increasing North Korea's nuclear warhead stockpile and improving its ballistic missile technology; for example, North Korea conducted three launches in 2024 of what it claimed were IRBMs equipped with maneuverable, hypersonic payloads.

- Kim seeks to intimidate the United States and its allies into abandoning opposition to North Korea's nuclear weapons and its aggression toward South Korea. For example, he responds to U.S. military planning with South Korea and trilateral cooperation with South Korea and Japan by ordering missile launches and threatening nuclear retaliation.

- North Korea will continue to defy international sanctions and engage in illicit activities, including stealing cryptocurrency, sending labor overseas, and trading UN-proscribed goods to resource and fund Kim's priorities, including ballistic missiles and WMD.

Kim will act aggressively to counter activities he views as undermining the regime and threaten to use force when he perceives U.S. and allied actions as challenging North Korea's sovereignty, undermining his power, or aiming to curb his nuclear and missile ambitions. Pyongyang is expanding its capacity for coercive operations and using new tactics as it becomes more confident in its nuclear deterrent. Since coming to power, Kim generally has relied on non-lethal coercive activities, including missile demonstrations and cross-border balloon launches of refuse, to win concessions and counter U.S. and South Korean military, diplomatic, and civilian activities.

- North Korea uses threats to try to stop South Korean efforts to disseminate information in the North, which he views as destabilizing his control. Kim in the past has challenged South Korea's de facto maritime boundary claims and may do so again, raising the prospects of renewed clashes along the Northern Limit Line.

- Kim could escalate to more lethal asymmetric activities if he judged North Korea's efforts at deterrence were not working and he needed to send a stronger message. He also could resort to these lethal activities if he believed doing so would intimidate South Korea or the United States into changing its policies to be more favorable to the North while minimizing the risk of retaliation.

WMD

Kim remains committed to increasing the number of North Korea's nuclear warheads and improving its missile capabilities to threaten the Homeland and U.S. forces, citizens, and allies, and to weaken U.S. power in the Asia-Pacific region, as evidenced by the pace of the North's missile flight tests and the regime's public touting of its uranium enrichment capabilities. North Korea is probably prepared to conduct a nuclear test and continues to flight test ICBMs so Kim can threaten the Homeland. Russia is increasingly supporting North Korea's nuclear status in exchange for Pyongyang's support to Moscow's war against Ukraine.

North Korea maintains its CBW capabilities and may use such weapons in a conflict or in an unconventional or clandestine attack against the United States or its allies.

Military

North Korea's military poses a lethal threat to U.S. forces and citizens in South Korea and the region by its ability to launch massive conventional strikes across the DMZ and continued investment in niche capabilities designed to deter outside intervention and offset enduring deficiencies in the country's conventional forces. The North's conventional military capabilities also provide Kim with options to advance his political objectives through coercion.

- The North Korean military would struggle to execute combined-arms maneuver warfare because its ground, air, and navy forces remain heavily reliant on Soviet-era equipment and lack adequate training, despite the investments to improve conventional capabilities.

- Kim will continue to prioritize efforts to build a more capable missile force—from cruise missiles to ICBMs and hypersonic glide vehicles—designed to evade U.S. and regional missile defenses, improve the North's precision strike capabilities, and put U.S. and allied forces at risk.

Pyongyang is positioned to gain technical expertise for its weapons developments in exchange for its munitions sales to Moscow, which could accelerate North Korea's testing and deployment efforts. Combat experience in the Russia-Ukraine war also could help Pyongyang strengthen its training and become more tactically proficient.

Cyber

North Korea is funding its military development—allowing it to pose greater risks to the United States—and economic initiatives by stealing hundreds of millions of dollars per year in cryptocurrency from the United States and other victims. Looking forward, the North may also expand its ongoing cyber espionage to fill gaps in the regime's weapons programs, potentially targeting defense industrial base companies involved in aerospace, submarine, or hypersonic glide technologies.

North Korea's Challenges

North Korea will continue to struggle overcoming the damage Kim's need for absolute control and aggressive policies—and the isolation these create—does to the country's economic strength and viability. Kim has so far been able to advance his WMD and missile programs and continue to threaten his neighbors and the United States, but this has come at the expense of his people and the country's overall health. The regime's recentralization campaign is meant to ensure the long-term survival of Kim family rule, but its periodic crackdowns restrict economic activity, threaten livelihoods, and promote inefficient state controls, contributing to food shortages and eroding civil order because of the violent crime they increasingly encourage.

Kim will struggle to reduce North Korea's dependence on China—in particular, for access to international banking and imports of critical raw materials, consumer goods, food, and the regime's crude oil supply—and withstand the influence this gives Beijing.

ADVERSARIAL COOPERATION

Cooperation among China, Russia, Iran, and North Korea has been growing more rapidly in recent years, reinforcing threats from each of them individually while also posing new challenges to U.S. strength and power globally. These primarily bilateral relationships, largely in security and defense fields, have strengthened their individual and collective capabilities to threaten and harm the United States, as well as improved their resilience against U.S. and Western efforts to constrain or deter their activities. Russia's war in Ukraine has accelerated these ties, but the trend is likely to continue regardless of the war's outcome. ***This alignment increases the chances of U.S. tensions or conflict with any one of these adversaries drawing in another. China is critical to this alignment and its global significance, given the PRC's particularly ambitious goals, and powerful capabilities and influence in the world.***

U.S. adversaries' cooperation has nevertheless been uneven and driven mostly by a shared interest in circumventing or undermining U.S. power, whether it be economic, diplomatic, or military. Concerns over escalation control and directly confronting the United States, as well as some divergent political interests, have tempered the pace and scope of these relationships. The leaders, though, are likely to continue to look for opportunities to collaborate, especially in areas in which there are mutual advantages and they lack other ways of achieving their aims toward or resisting the United States alone.

Russia has been a catalyst for the evolving ties, especially as it grows more reliant on other countries for its objectives and requirements including in but not limited to Ukraine. Moscow has strengthened its military cooperation with other states, especially Pyongyang and Tehran. Russia also has expanded its trade and financial ties, particularly with China and Iran, to mitigate the impact of sanctions and export controls.

- The PRC is providing economic and security assistance to Russia's war in Ukraine through support to Moscow's defense industrial base, including by providing dual-use material and components for weapons. China's support has improved Russia's ability to overcome material losses in the war and

launch strikes into Ukraine. Trade between China and Russia has been increasing since the start of the war in Ukraine, helping Moscow to withstand U.S. sanctions.

- Iran has become a key military supplier to Russia, especially of UAVs, and in exchange, Moscow has offered Tehran military and technical support to advance Iranian weapons, intelligence, and cyber capabilities.

- North Korea has sent munitions, missiles, and thousands of combat troops to Russia to support the latter's war against Ukraine, justified as fulfilling commitments made in the Treaty on Comprehensive Strategic Partnership that Pyongyang and Moscow announced in June 2024.

Cooperation between China and Russia has the greatest potential to pose enduring risks to U.S. interests. Their leaders probably believe they are more capable of countering perceived U.S. aggression together than alone, given a shared belief that the United States is seeking to constrain each adversary.

- For at least a decade, Beijing and Moscow have used high-profile, combined military activities primarily to signal the strength of the China–Russia defense ties. This relationship has deepened during the Russia-Ukraine war, with China providing Russia dual-use equipment and weapons components to sustain combat operations.

- Russia has increased its oil and liquefied natural gas (LNG) exports to China in an effort to maintain revenues in the face of sanctions by Western states.

- China is using its increased cooperation with Russia to attain a stronger presence in the Arctic and legitimize its influence there. One area of cooperation is China's production of icebreaker ships that enable safe passage through Arctic waters.

- The two countries probably will expand combined bomber patrols and naval operations in the Arctic theater to signal their cooperation and make it more concrete. In November, they also agreed to expand their cooperation on developing the NSR for its economic potential and as an alternative to Western dominated routes.


OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA
UNITED STATES INTELLIGENCE COMMUNITY

POLITICS | NATIONAL SECURITY

FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale

Christopher Wray warns that pre-positioned malware could be triggered to disrupt critical systems in the U.S.

By Joe Parkinson Follow *and Drew Hinshaw* Follow

Feb. 18, 2024 1:49 pm ET

FBI Director Christopher Wray KEVIN DIETSCH/GETTY IMAGES

MUNICH—As intelligence chiefs and policymakers gathered for this city's annual security conference focused on the wars in Ukraine and the Middle East, the director of the Federal Bureau of Investigation urged them not to lose sight of another threat: China.

Christopher Wray on Sunday said Beijing's efforts to covertly plant offensive malware inside U.S. critical infrastructure networks is now at "a scale greater than we'd seen before," an issue he has deemed a defining national security threat.

Citing Volt Typhoon, the name given to the Chinese hacking network that was revealed last year to be lying dormant inside U.S. critical infrastructure, Wray said Beijing-backed actors were pre-positioning malware that could be triggered at any moment to disrupt U.S. critical infrastructure.

"It's the tip of the iceberg...it's one of many such efforts by the Chinese," he said on the sidelines of the security conference that has been dominated by questions over Ukraine and the death of Russian opposition leader Alexei Navalny. China, he had earlier told delegates, is increasingly inserting "offensive weapons within our critical infrastructure poised to attack whenever Beijing decides the time is right."

The FBI chief declined to elaborate on what other critical infrastructure had been targeted, stressing that the Bureau had "a lot of work under way."

Wray's comments are the latest in a string of public warnings by senior Biden administration officials to animate their fears about China's advanced and well-resourced hacking prowess. Western intelligence officials say its scale and sophistication has accelerated over the past decade. Officials have grown particularly alarmed at Beijing's interest in infiltrating U.S. critical infrastructure networks, planting malware inside U.S. computer systems responsible for everything from safe drinking water to aviation traffic so it could detonate, at a moment's notice, damaging cyberattacks during a conflict.

The director has been prodding foreign governments in Europe and Asia to increase resources on the threat of Chinese hacking campaigns, particularly protecting critical infrastructure. He described the response as gratifying and a step change from several years ago when some were still skeptical about the Chinese cyber threat.

In California, Wray met with counterparts from the Five Eyes intelligence community —which encompasses the U.S., Australia, New Zealand, Canada and the U.K.—to share respective strategies for cyber defense; he has also traveled to Malaysia and India to discuss China's hacking campaign with authorities in both countries.

"I am seeing more from Europe," he said. "We're laser focused on this as a real threat and we're working with a lot of partners to try to identify it, anticipate it and disrupt it."

The Netherlands' spy agencies said earlier this month that Chinese hackers had used malware to gain access to a Dutch military network last year. The agency, considered to have one of Europe's top cyber capabilities, said it made the rare disclosure to show the scale of the threat and reduce the stigma of being targeted so allied governments can better pool knowledge.

Beijing routinely denies any accusations of cyberattacks and espionage linked to or backed by the Chinese state and has accused the U.S. of mounting its own cyberattacks. But evidence of a Chinese state-backed program has been building in recent years and the U.S. has charged a string of officers from the People's Liberation Army cyber units with stealing secrets.

Wray said the U.S. is particularly focused on the threat of pre-positioning, which some European officials have described as the cyber equivalent of pointing a ballistic missile at critical infrastructure.

A report released this month by agencies including the FBI, the Cybersecurity and Infrastructure Agency and the National Security Agency said Volt Typhoon hackers had maintained access in some U.S. networks for five or more years, and while it targeted only U.S. infrastructure directly, the infiltration was likely to have affected "Five Eyes" allies.

The Justice Department and FBI took action in December after obtaining court approval to dismantle a botnet, or network of hacked devices, consisting of small office and home office, or SOHO, routers. Mostly from Cisco or Netgear, the routers were vulnerable because they had reached so-called end-of-life status, meaning they were no longer receiving routine security updates from the manufacturers.

Those attacks are now being amplified by artificial intelligence tools, Wray said.

"The word 'force multiplier' is not really enough," he said.

Machine learning translation has helped Chinese security operatives to more plausibly recruit assets, steal secrets and rapidly process more of the information they are collecting, the director said.

"They already have built economic espionage and theft of personal and corporate data as a kind of a bedrock of their economic strategy and are eagerly pursuing AI advancements to try to accelerate that process," he said.

Write to Joe Parkinson at joe.parkinson@wsj.com and Drew Hinshaw at drew.hinshaw@wsj.com

Appeared in the February 20, 2024, print edition as 'FBI Director Issues Warning on China Cyberattacks'.

Further Reading

Chinese Spies Hit More Than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals

Videos

https://www.wsj.com/opinion/the-first-large-scale-cyberattack-by-ai-4a1e1a30

OPINION COMMENTARY Follow

The First Large-Scale Cyberattack by AI

With basic tech and little human oversight, Chinese spies apparently exploited Anthropic's Claude Code.

By Nury Turkel

Nov. 23, 2025 12:03 pm ET

GETTY IMAGES

A state-backed threat group, likely Chinese, crossed a threshold in September that cybersecurity experts have warned about for years. According to a report by Anthropic, attackers manipulated its AI system, Claude Code, to conduct what appears to be the first large-scale espionage operation executed primarily by artificial intelligence. The report states "with high confidence" that China was behind the attack.

AI carried out 80% to 90% of the tactical operations independently, from reconnaissance to data extraction. This espionage campaign targeted roughly 30 entities across the U.S. and allied nations, with Anthropic validating "a handful of successful intrusions" into "major technology corporations and government agencies."

GTG-1002—Anthropic's designation for this threat group—indicates that Beijing is unleashing AI for intelligence collection. Unless the U.S. responds quickly, this will be

the first in a long series of increasingly automated intrusions. For the first time at this scale, AI didn't merely assist in a cyberattack but conducted it.

Traditional cyber-espionage requires large teams working through reconnaissance, system mapping, vulnerability identification and lateral movement. A sophisticated intrusion can take days or weeks. China compressed that timeline dramatically through AI automation. The attackers manipulated Claude into functioning as an autonomous cyber agent, with the AI mapping internal systems, identifying high-value assets, pulling data and summarizing intelligence before human operators made decisions.

The attackers bypassed Claude's safety systems through social engineering, convincing the AI they were legitimate cybersecurity professionals conducting authorized testing. By presenting malicious tasks as routine security work, they manipulated Claude into executing attack components without recognizing the broader hostile context.

An important limitation emerged: Claude frequently overstated findings and fabricated results, claiming credentials that didn't validate or presenting publicly available information as critical discoveries. This AI hallucination problem remains a significant obstacle to fully autonomous cyberattacks—at least for now.

Most striking is what China didn't need. GTG-1002 didn't rely on cutting-edge malware or expensive proprietary tools. It used common open-source penetration-testing frameworks orchestrated through Model Context Protocol servers. Beijing hasn't only upgraded its toolkit; it has replaced the craftsman with the assembly line. Capabilities once reserved for well-resourced intelligence agencies can now be replicated by smaller actors using widely available technology.

It also reveals a deeper strategic dynamic. China is spying with AI and spying on American AI. Beijing is studying how U.S. models behave, where they fail, and how they can be manipulated. Every malicious query becomes training data for China's systems.

Anthropic deserves credit for disclosing the incident publicly and working with U.S. authorities. That transparency should set an industry standard. But the disclosure underscores a larger problem: Current safeguards aren't designed for adversarial actors that move at machine speed.

The response must be urgent and clear. AI misuse can't be treated as a narrow cyber issue; it is now central to the broader technology competition with China. Five responses are necessary:

First, AI-assisted defense must become standard across federal agencies, critical infrastructure and major corporations. AI can detect anomalies in real time and accelerate incident response from hours to minutes. China is using AI to accelerate attacks. The U.S. must use AI to accelerate defense.

Second, companies must disclose incidents of AI misuse within 72 hours. When AI systems are manipulated into performing malicious actions, critical details must be shared: attack vectors, guardrail failures, and forensic signatures that might help others detect similar intrusions. Without mandatory disclosure backed by safe-harbor provisions, businesses will keep quiet to avoid reputational damage. Policymakers can't craft effective rules if the private sector conceals the incidents that illuminate emerging risk.

Third, AI companies must embrace secure-by-design principles. As Anthropic's report warns, the techniques used by GTG-1002 will proliferate. The next generation of AI models must incorporate robust identity verification, real-time monitoring for malicious behavior, and guardrails resilient to social-engineering prompts.

Fourth, the U.S. and its allies need international norms governing AI-enabled cyber operations. Existing frameworks were created before autonomous systems existed. If Washington doesn't shape these norms and lead, Beijing will.

Fifth, the U.S. must modernize how it shares threat intelligence. AI-accelerated attacks unfold too quickly for traditional bureaucratic information-sharing mechanisms. We need automated real-time systems capable of disseminating alerts across sectors in hours, not weeks.

The first AI-driven cyberattack is the opening act of a new era. GTG-1002 should be remembered the way we recall the first internet worm or the first ransomware wave: as an inflection point.
The cyber cold war just went kinetic. The weapons fire themselves now.

The question isn't whether adversaries will continue exploiting AI for offensive operations. They will. The question is whether the U.S. will act quickly enough to defend itself.

China has signaled its ambitions. GTG-1002 shows it is already acting on them. The U.S. must stop debating the future of AI-enabled aggression and begin preparing for the conflict that has already arrived.

Mr. Turkel is a lawyer specializing in global trade compliance, export controls, sanctions and anticorruption compliance. He is author of "No Escape: The True Story of China's Genocide of the Uyghurs."

Appeared in the November 24, 2025, print edition as 'The First Large-Scale Cyberattack by AI'.

December 2, 2025

The Honorable Bob Latta
Chair, House Energy & Commerce Committee Subcommittee on Energy
The Honorable Kathy Castor
Ranking Member, House Energy & Commerce Committee Subcommittee on Energy
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Latta and Ranking Member Castor,

I am writing to you relating to today's hearing by the Energy Subcommittee entitled "Securing America's Energy Infrastructure: Addressing Cyber and Physical Threats to the Grid." This is a critical problem that does not get enough attention, and I appreciate the Subcommittee holding a hearing on the issue. My name is Desmond Wheatley, and I serve as the CEO of Beam Global (Beam).

Beam Global (Nasdaq:BEEM) is an American company and is a leading provider of innovative products and technologies for energy storage, energy security, smart cities infrastructure and the electrification of autonomous vehicles, drones and other transportation. Beam's patented EV ARC™ is the only 100% off-grid, transportable, rapidly deployed energy generation and storage option for energy security and the electrification of transportation on the market. It can be installed in minutes to provide highly robust and scalable electrical infrastructure where and when needed without any construction or electrical work and without relying on the utility grid. It is made in America and continues to provide electricity in hurricanes and in flooding of up to nine feet.

Beam has a significant interest in ensuring that the nation's centralized electric grid can meet critical challenges it currently faces due to unprecedented increased demand for electricity due to rapid growth in many industrial sectors such as AI, data centers and the electrification of industry and transportation. The combination of increased demand and the reliance on centralized electricity infrastructure makes the American economy and public well-being increasingly vulnerable to grid failure, whether from capacity-driven outages, severe weather events or from cyber and kinetic attacks. As we push for the electrification of nearly everything in our life, identifying creative solutions is critical. Luckily, we can get direction from a different energy crisis a half a century ago.

In 1975, in the aftermath of an oil crisis, President Ford signed an act which led to the creation of the Strategic Petroleum Reserve (SPR). The U.S. has relied on the SPR for decades. The SPR serves as a safety net for the U.S., ensuring that there will not be a crisis that leaves Americans without oil.

We have entered an era where electricity is increasingly becoming the lifeblood of our society, powering everything from critical infrastructure to daily conveniences. While much time, money and effort have been put towards improving the existing electric grid, the Federal Energy Regulatory Commission (FERC) found in 2014 that the destruction of nine critical substations and one transformer manufacturer would cause a total collapse of the U.S. electrical grid resulting in a blackout that could last for about 18 months.

Consider the impacts such a blackout would have on American wellbeing in 2025. Loss of life, an economic landslide, and a complete breakdown of our communications systems are all but certain. Even our transportation system is relying more on the centralized grid.

Threats to our grid should not be perceived by the American public as just a hypothetical scenario. For example, in the early weeks of Russia's invasion of Ukraine in 2022, U.S. grid operators were targeted by the infamous Russian-led "PIPEDREAM" malware attack, which some security experts determined was the closest U.S. grid infrastructure has come to going down. At the same time, suspected foreign bad actors were joined by home-grown attackers. Shootings in North Carolina knocked out power for 45,000 people in December of 2022, shortly after around 14,000 Washingtonians lost power when four substations were vandalized. In 2022 federal authorities thwarted an attempt from extremists to use assault weapons to bring down the grid in Baltimore, which, had it not been prevented, would have set off a cascade of power failures.

All of this is to say that the risks to, and vulnerabilities of, our centralized American grid cannot be ignored. Creative solutions to strengthen grid resiliency and provide a strategic backbone must be pursued by our elected officials in Washington D.C. That is why I am calling on Congress and the Trump Administration to create a Strategic Electric Reserve (SER).

Unlike its oil counterpart, such a reserve should adopt a decentralized model, consisting of independent energy nodes which operate independently of the grid and provide an extra layer of electricity generation and delivery. Each node should function autonomously, generating, storing, and delivering electricity independent of the centralized grid and located where electricity is needed most such as for first responders, food and water infrastructure, healthcare and government facilities. This would ensure a distributed and resilient network that can withstand localized disruptions without compromising the broader electricity supply. An SER would provide robust backup, immune to centralized failures, cyber threats, and external attacks. This is not a question of hardening the existing grid which will still be vulnerable to centralized failure. This is about creating an extra layer of completely independent micro generation and storage to power critical needs during a failure of the centralized grid.

Creating the SER will not be an easy task. Energy companies, utility companies, state public utility commissions, and large users such as AI companies and data center providers, car companies, and federal agencies, must work together in the development of the SER. It will require bold leadership from government and industry.

In addition to establishing independent energy nodes that add redundancies to the existing electrical grid, the SER would also add critical capacity to the grid but without taking the decades that the building of power stations and transmission and distribution infrastructure require. It could also address specific needs in areas where costs and geography make electricity deployment challenging, especially in traditionally underserved rural and low-income areas. Including Build America/Buy America requirements would have the added bonus of ensuring domestic manufacturing standards and job creation, while promoting independence from foreign supply chains. I believe it would spur a next-generation of American innovation.

From data centers to military operations, healthcare, and transportation, every facet of American life requires a secure and stable source of electricity. The existing grid, challenged by escalating demand and susceptible to disruptions caused by lack of capacity, extreme weather and malicious attacks, poses a considerable national security risk. According to the Department of Energy, grid interruptions already cost U.S. businesses around $200 billion a year in lost productivity and related costs. As the U.S. becomes increasingly reliant on a reliable and robust supply of electricity, we can only expect that number to grow. Establishing the SER will help combat these challenges by serving as a decentralized, resilient, and redundant system capable of ensuring uninterrupted electricity supply even in the face of security threats and grid failures.

The SER is not the only answer to these problems, but it adds a critical layer of security and redundancy that the current centralized national and regional grids cannot offer. It is for these reasons that Congress and the Trump Administration should take action to address the vulnerabilities of the existing electrical grid and chart a course towards a more secure, reliable, and equitable energy landscape for all Americans. As the nation transitions towards an electrified future, the Strategic Electric Reserve stands as a beacon of preparedness, safeguarding the vitality of our society in the face of evolving challenges.

It is time for Congress to create and the Trump Administration to implement a Strategic Electric Reserve.

Thank you,

Desmond Wheatley
CEO Beam Global

/S/ Desmond Wheatley