Testimony of Frank Cilluffo

Director

McCrary Institute for Cyber and Critical Infrastructure Security

Auburn University

House Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland."

Tuesday, January 13, 2026

Good morning, Chairman Ogles, Ranking Member Swalwell, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today on behalf of the McCrary Institute for Cyber and Critical Infrastructure Security at Auburn University. I appreciate the Subcommittee's leadership in examining how the United States can more effectively deter and disrupt malign cyber activity targeting the homeland.

Last month, the McCrary Institute released a task force report directly relevant to today's hearing, *U.S. Cyber Policy: Offense, Deterrence, and Strategic Competition*. I had the privilege of co-chairing this effort alongside Chris Inglis, our nation's first National Cyber Director; General Frank McKenzie, former Commander of U.S. Central Command; and Tom Bossert, former Assistant to the President for Homeland Security. This report draws on extensive operational, policy, and intelligence experience of our national security and law enforcement task force to examine how U.S. cyber policy must adapt to persistent strategic competition.

At a time when our geopolitical adversaries and transnational criminal organizations across the world are creating digital havoc, the committee is rightly asking a fundamental question: how can the U.S. more credibly deter adversaries in cyberspace and what does that require for homeland security and domestic preparedness? The question is especially urgent in the age of AI—a topic I know you are examining carefully—which is accelerating both adversary tradecraft and the speed at which cyber operations can translate into real-world effects. I appreciate your understanding that offensive cyber capabilities have inherently defensive implications for cybersecurity in the homeland.

This challenge has grown more acute as adversaries expand their capabilities, embed disruptive access within U.S. critical infrastructure, and exploit gaps between military, intelligence, law enforcement, and civilian authorities. What began in the early 2000s as an intelligence-driven model centered on clandestine collection has evolved into a contested operational environment where cyber effects are now entwined with traditional military planning, economic coercion, and crisis escalation dynamics. We saw this dynamic recently in the U.S. operation in Venezuela, where reporting indicates cyber activity was layered with space, military aircraft, unmanned systems, and intelligence assets.

The United States must now navigate this environment using frameworks that were not designed for the scale, persistence, or tempo of today's threats, while relying on an organizational structure that reflects both institutional strengths and enduring policy and operational friction. The result is a posture that too often emphasizes episodic responses rather than sustained advantage in an environment defined by continuous contact.

Over the last decade, U.S. adversaries—including Russia, China, Iran, and North Korea—have steadily expanded the scope, sophistication, and ambition of their offensive cyber operations. Among them, China has demonstrated the clearest long-term strategic intent. Beijing's campaigns targeting U.S. government networks, defense industrial base entities, and privately owned critical infrastructure underscore a preference for persistent access rather than short-term disruption. These operations are designed less for immediate disruption than for strategic leverage—pre-positioning capabilities that could be exercised to coerce, deter, or delay U.S. decision-making during a crisis.

Recent campaigns such as Volt Typhoon and Salt Typhoon represent a significant evolution in this approach. Rather than focusing solely on data theft, these operations target operational technology and infrastructure networks, blurring the line between espionage and preparation of the battlefield. This activity should be understood not as isolated incidents, but as part of a broader strategy of continuous engagement aimed at shaping the strategic environment well in advance of conflict.

Russia, for its part, has demonstrated how cyber operations can be integrated directly into military campaigns. In Ukraine, destructive malware, information operations, and cyber-enabled disruption of critical services accompanied conventional military assaults. These actions reinforce the reality that adversaries increasingly view cyberspace as a domain that is always "on"—one in which access, influence, and coercive leverage are cultivated over time rather than activated only at the moment of crisis.

Against this backdrop, U.S. cyber operational policy has undergone an important shift. For many years, offensive cyber activity was tightly centralized, often requiring extensive interagency deliberation and senior-level approval. This changed with the issuance of National Security Presidential Memorandum 13 in 2018, which allowed the President to delegate greater operational decision-making authority to designated organizations, most notably U.S. Cyber Command. At the same time, the Department of Defense formally adopted the concept of "defend forward," recognizing that the United States must operate persistently in foreign networks to disrupt adversary campaigns before they reach U.S. targets.

This shift has yielded meaningful operational benefits. However, it has also reignited unresolved questions regarding oversight, intelligence equities, and the strategic risks associated with persistent engagement. These are not theoretical concerns. They go to the heart of how the United States balances operational agility with democratic accountability and strategic stability. Moreover, these evolutions in how offensive cyber is conducted has created implications for our defensive posture and how the federal government works with stakeholders like the private sector to prepare for and defense against threats.

Importantly, offensive cyber operations alone are not sufficient to protect the homeland. When cyber action is taken abroad, it is incumbent upon the Department of Homeland Security—particularly through the Cybersecurity and Infrastructure Security Agency—to defend domestic networks and work with critical infrastructure owners and operators to improve resilience across sectors. This mission is essential to homeland security, economic stability, and public confidence. Our adversaries increasingly seek to impose domestic costs as a means of deterring the United States from advancing its interests abroad or honoring its commitments to allies.

To meet these challenges, the United States must strengthen the doctrinal, legal, and organizational foundations of its cyber strategy. This includes clarifying interagency roles and responsibilities, improving mechanisms for information sharing with trusted private-sector partners, and ensuring that resilience and security are treated as core elements of deterrence—not afterthoughts. It also requires refining deterrence frameworks to account for adversaries who deliberately blend espionage, coercion, influence operations, and pre-positioning activity below the threshold of armed conflict.

But just as offense alone is insufficient, so too, would be a purely defensive posture. Simply put: We cannot firewall our way out of this problem. U.S. cyber policy must move beyond reactive, episodic responses and toward a durable posture capable of operating effectively in an era of continuous foreign intrusion. We should not rely on authorities and assumptions built for a different era. Strategic competition in cyberspace demands sustained engagement, clearer governance, and a realistic appreciation of how offensive and defensive actions interact to shape adversary behavior.

The vast majority of critical infrastructure is owned and operated by private entities, placing them on the front lines of strategic competition in cyberspace. Yet current policy too often treats these actors as passive victims rather than as potential partners in defense. As our report notes, effective deterrence in cyberspace depends not only on government action, but on enabling trusted private-sector operators to take timely, proportionate, and lawful steps to detect, disrupt, and eject malicious activity from their networks. Clarifying the legal and policy boundaries around active cyber defense—while preserving strong oversight and safeguards—would strengthen collective defense, raise adversary costs, and reduce the burden on federal authorities alone to secure the homeland.

Many of the capabilities relevant to modern cyber conflict, such as threat intelligence collection, rapid incident response, and the ability to deploy deception or interdiction tools at scale, reside not within government networks but inside major technology firms, cloud providers, and critical infrastructure operators. Private entities already perform elements of active defense by hunting adversaries within their systems, deploying beacons, mitigating malicious traffic, and collaborating with federal agencies during botnet takedowns.[1]

[1] "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats," October 2016, Active Defense Task Force, Center for Cyber and Homeland Security, The George Washington University, accessed December 6, 2025, < https://cpb-us-e2.wpmucdn.com/wordpress.auburn.edu/dist/8/7/files/2021/01/into-the-gray-zone.pdf>.

Although these actions fall short of offensive operations in the traditional sense, they demonstrate how the private sector can seek to shape adversary behavior and deny operational freedom through forward-leaning measures that are lawful, risk-calibrated, and technically sophisticated. What remains unresolved is how far private actors should be permitted to go when defending their networks from state-sponsored threats, and how the government should structure oversight, liability protections, and coordination frameworks to ensure that such activity enhances national security without triggering escalation or infringing on civil liberties. As adversaries increasingly target U.S. companies to gain strategic leverage, the question is not whether the private sector will play a role in active cyber defense, but whether that role will be integrated into a coherent national strategy or continue to evolve in an ad hoc and legally ambiguous "gray zone."

Initiatives such as CISA's Joint Cyber Defense Collaborative and the NSA's Cybersecurity Collaboration Center are positive steps towards operationalizing collaboration between government and the private sector. It is vital that critical infrastructure owners and operators have the right relationships and partners in government to understand the threat and improve resiliency. This is the sort of active cyber defense we need to build on, in conjunction with a more assertive offensive stance.

It is a national security imperative that federal, state, local, tribal, territorial, and private sector partners cooperate in new and robust ways to minimize potential future operational disruptions and sensitive data compromises. Lastly, the threat posed by the adversaries like the typhoon actors is not merely a cybersecurity challenge but should be looked at as a broader threat to the United States and its allies. As the PRC develops new ways to undermine U.S. national security, it is critical to adopt a whole-of-government approach to countering such threats.

The stakes are significant. As adversaries deepen their access into American networks, the United States must decide whether its cyber strategy will remain constrained by outdated frameworks or evolve to reflect the realities of twenty-first-century conflict. Congress has a critical role to play in that recalibration—by modernizing authorities, strengthening oversight, and ensuring that our institutions are equipped to operate with both agility and accountability.

Mr. Chairman, this concludes my prepared remarks. I look forward to your questions and to working with the Subcommittee to strengthen the security and resilience of the United States in cyberspace.

Testimony Of

Drew Bagley
CrowdStrike

Before

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland"

January 13th, 2026

Chairman Ogles, Ranking Member Swalwell, members of the subcommittee, thank you for the opportunity to testify today. Throughout my career, I have seen firsthand the challenges and opportunities of improving American cybersecurity from my work in the private sector, government, and academia. For more than a decade at CrowdStrike, a leading cybersecurity company, I have had a front row seat to cybersecurity innovation while building our privacy and public policy programs and advising customers around the globe. Prior to that I worked at the intersection of law and technology in the FBI's Office of the General Counsel. I previously taught at universities in the US and Europe, and currently serve as an adjunct professor in American University's cybersecurity policy program.

As a leading U.S. cybersecurity company, CrowdStrike has a useful and often quite textured vantage point on malicious activities in cyberspace. Protecting organizations with our cybersecurity technology, threat intelligence, professional services offerings and incident response work, we confront a full range of cyber threats. We defend many components of the U.S. Federal government and serve as a commercial cybersecurity provider for major technology companies, 8 of the top 10 financial services firms, and 43 of 50 U.S. states[1]; as well as all manner of critical infrastructure entities and small and medium sized businesses. We defend America.

Nation states are relentless. In parallel, there is a democratization of destruction whereby those perpetrating cyber attacks no longer need the knowledge, resources, or time once required to execute high impact attacks–indeed, adversaries can "vibehack" their way to success. Moreover, because legitimate credentials may be purchased in online criminal forums, along with the tools to deploy ransomware and malware, the means to attack are available for those who merely have the intent. As adversaries evolve, defenders are most successful when they adapt. This holds true for our digital ecosystem in general. As we adopt new technologies, features and abilities, we must

[1] State and Local Governments, CrowdStrike.
https://www.crowdstrike.com/en-us/solutions/state-local-government/

adapt how we secure them. Today, this means we must think about how we detect, prevent, and defend an attack surface that now includes AI.

To what extent is America secure from cyberthreats?
America remains vulnerable to cyberattacks, and the scope and severity of which continues to increase.[2] To be clear, some organizations are effectively defending themselves. Bright spots include broader adoption of modern endpoint and managed security solutions in public and private enterprises. Still, organizations face an array of attacks targeting cloud environments, Software as a Service (SaaS) applications, and identities.

Under-resourced public institutions and small and medium sized businesses are particularly vulnerable. But high-profile attacks over the past few years from China, notably the VANGUARD PANDA/Volt Typhoon attacks targeting critical infrastructure and the OPERATOR PANDA/Salt Typhoon attacks targeting telecommunications entities have raised the most acute concerns from a national security perspective. Despite significant investment in cybersecurity measures, the status quo isn't working.

What's gone wrong?
Simply put: threat actors are still operating at scale, still operating with limited consequences, and still all-too-often achieving their objectives. They are still seeing a clear return on investment. They are still assessing a risk calculus that shows favorable outcomes. To make durable progress, we must work in a concerted fashion to change each of these conditions. (I describe how below.)

What's the role for "offense" in confronting cyber threats?
In the cyber context, offense can mean a number of different things. At a high level, from a law enforcement or industry lens, threat actor infrastructure disruptions might include seizing malicious domains, servers, or relay infrastructure; asserting control over hosted malware kits or botnets; or offlining darkweb forums or sites used to anonymously host pilfered information. Importantly, denying an adversary the ability to monetize their efforts is also achievable. At a minimum, these sorts of operations require careful planning, pose coordination challenges, and may raise questions about burden sharing.

Offense from a military or intelligence lens might imply breaching foreign organizations or otherwise attacking them, such as through denial of service or destructive attacks. The latter can focus on deleting data, destroying IT systems, or causing 'effects' in the real world, such as by manipulating operational technology (OT) systems and thus associated infrastructure.

At the level of the enterprise, we advocate that defenders threat hunt or work with a partner who can do it on their behalf. This essential practice can be performed on each organizations' own

[2] America's technology infrastructure consists of an array of IT, OT, telecommunications, cloud and digital services, cyber-physical systems, and the data and identity layers that connect them all. These systems are managed by organizations large and small, well-resourced and under-resourced.

systems, resources, and data.[3] Therefore, it's mainly a proactive approach–sometimes called active defense–rather than offense per se. But threat hunting is one of the most effective techniques we have as an industry to confront targeted attacks.

Should cyberattack victims or their representatives "hack back"?
When the 'hack back' policy discourse started in earnest about 15 years ago, it was in response to multiple reports of egregious campaigns where adversaries had, for example, breached a series of organizations like National Labs or defense contractors, exfiltrated gigabytes of sensitive data, left that data on a fairly exposed staging server, and collected it later at their convenience. In that type of scenario, particularly where the victim(s) possessed relevant forensic artifacts and telemetry, the inability to legally "do something," often meaning to delete the only copy of the stolen data, caused a great deal of consternation.

Today, attacks are generally far more sophisticated, leveraging compromised accounts of legitimate (e.g., SaaS) applications; transient, ephemeral, or shared cloud environments; and other obfuscation techniques. In this environment, a policy framework that's more conducive to 'hack back' operations carried out by a broad array of actors could yield revictimization, collateral damage, and impacts to innocent victims. Ongoing investigations could be disrupted. Retaliation could lead to waves of escalation, potentially along geopolitically-salient lines. For these reasons, we share the view that offense is best left to professionals with relevant authorities, deconfliction processes, and clear oversight. A democratized regime for hacking back that lacks these attributes probably creates more problems than it solves.

Is defense discredited?
No. Defense is foundational. Even those who wish to increase offense must recognize the value of robust defenses. Even if a city announced an enormous and well-resourced crackdown on crime, homeowners should still, rationally, take the basic steps of shutting and locking their doors at night. New threat actors emerge routinely with different capabilities and motivations. Economic and geopolitical conditions change, often for the worse. Having defenses in place amid this changing terrain is essential. Further, to the extent policy dictates that offensive actions will increase, that should lead to a heightened, rather than reduced, focus on defense.

In the kinetic world, it is not uncommon to categorize 'soft' targets versus 'hard' targets. Simply put, organizations that have hardened themselves with modern approaches are more secure and have drastically reduced the likelihood of suffering a high impact event. Those that haven't remain vulnerable not only to infiltration but to existential impacts in the face of an incident.

It's often said that 'mom-and-pop' operations can't be expected to singlehandedly defeat the People's Liberation Army. That's true. National-level policies and capabilities are needed to create conditions of reduced threats. But, as with other threats, hazards, and risks, all organizations should take reasonable steps to defend themselves.

[3] As a vendor, we facilitate sharing of visibility in threat hunting operations at the sector-level, national-level, and international level through our threat intelligence reporting.

What's the role of deterrence in defeating threats?
Mechanically, deterrence is achieved either through denial (i.e., an adversary realizes an attack won't be effective, so they apply their energies elsewhere) or through a credible threat of retaliation. Retaliation can be intradomain (i.e., also a cyberattack) or crossdomain (e.g., leveraging a law enforcement or conventional military capability).[4]

Cyberattacks are caused by adversaries. Threats themselves aren't deterrable; the people, institutions, and nations behind them often are. The people in question are military or political figures. Or anonymous criminals. They might be rich or poor; empowered or desperate; or seeking fame or seeking to effectuate a radical political or social cause. They might be, in the political science sense, rational or irrational actors. Given that their conditions and motivations vary so widely, there is no singular approach to deterrence that could succeed.

Deterrence is difficult to measure. Clearly, a significant number of adversaries are not presently deterred. As a community, we must strengthen deterrence as part of a holistic approach to cyberdefense.

How should policymakers think about resourcing defense vs. offense?
Unfortunately, a simple 50-50 (or 80-20, or 20-80)-style-answer here is elusive. But several considerations should guide investments:

- With respect to defense, organizations should develop realistic, informed threat models and plan to confront those threats.
- Some amount of investment in security is reasonable. Against today's adversaries, unfortunately, basic hygiene and best practices alone fail. The ability to achieve real-time visibility, detection, and response across federated IT systems is required for protection and threat hunting. For organizations with resource constraints, clear illustrations depicting how investments map to reduced risks are typically most persuasive to planners, be they management, boards, or appropriators.
- Efficacy is often more important than resourcing overall. Unfortunately, in today's public policy debates, there are many false proxies for assessing whether cyber defenses are effective. Simply because the federal government, a particular sector, or an individual organization spends a certain dollar amount on security does not mean it is buying the best technology, deploying it on the most critical assets, or operating it correctly. Similarly, and especially in government, technology with the lowest price tag—or that is included as part of an add-on bundle—is unlikely to deliver the same security outcomes.
- Ultimately, it's probably reasonable to conceive of security investments as a portion of overall IT spending (best practices for which may vary, but are sometimes assessed by reputable technology research advisory firms).

[4] For our part, the core technologies we produce–namely the Falcon platform and associated capabilities–essentially seek to support denial. Our threat intelligence products, among other things, can support threat actor identification, which can strengthen targeting for organizations with enforcement and defense missions.

Similarly, at a national-level, it's appropriate and realistic for institutions operating under Title 10 and Title 50 authorities to resource offensive missions. But rather than defining resourcing levels for those activities relative to cyber *defense* investments, it's probably more reasonable for planners to consider cyber offense relative to other *offensive* capabilities (e.g., kinetic options) that might achieve a similar outcome.[5]

What roles, missions, and authorities must change to better confront cyber threats?
Our core prescription is bringing to bear more focused, more persistent, and more tightly-orchestrated campaigns disrupting threat actors and those who support them. This means leveraging more technical operations, erecting more barriers to success, and leveraging all available tools of statecraft (i.e., crossdomain responses) to pressure adversaries, dampen their success, and prevent them from operating at scale.

Consider first financially-motivated attacks, such as ransomware. CISA, probably acting through JCDC, should consult with industry to determine which groups are most problematic (either because of scale, targeting practices, or some other criteria) and establish a "Most Wanted"-style list. CISA should ascertain targeting information about those responsible from stakeholders.[6] They should orchestrate actions with relevant law enforcement partners (or, where appropriate, Intelligence Community partners) to use disruption authorities and, where possible, simultaneous enforcement actions to target those responsible. They should orchestrate actions with partners at Treasury and the private sector financial ecosystems to complicate or prevent cash-outs or monetization of hacking. They should leverage industry partners who can contribute along the way by sharing visibility and better enforcing their own terms of service, given that most firms already contractually prevent criminality and abuse.

Similar coordination must take place focused on nation state actors. In those cases, there might be less focus on disrupting monetization and law enforcement actions,[7] and more on Title 10 and Title 50 actions. Still, particular actions should be prioritized in consultation with relevant stakeholders and executed with great frequency.

[5] Whether other means to attain intelligence or other means to achieve effects.
[6] Our sense is that CISA possesses all relevant authorities to perform these actions. National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1715 (Joint Cyber Planning Office), 134 Stat. 3388 (2021).
[7] Although not in the case of national state actors engaged in cybercrime to fund the regime, such as the DPRK, and/or operating from 3rd party countries where U.S. and allied nations have law enforcement reach.

Everything I've described here does take place–just not nearly enough. It's really a matter of will for decisionmakers to demand that this sort of thing, which happens periodically, takes place routinely,[8] and on the highest impact targets.

How does the advancement of AI impact these considerations?
The advancement of AI does not materially impact threat actor motivations. It does, however, provide threat actors with a new class of systems to target, new infrastructure to leverage, and a new accelerant to automate their own TTPs. We expect this trend to continue as adversaries exploit new tools and adapt to changing conditions.

AI itself is under threat from adversaries, whether its the systems, data, or human and non-human identities or the end user platform. This will only increase as AI becomes more ubiquitous and disappears into the traditional IT stack, becoming a commonplace part of America's digital infrastructure. Much like the need for detection and response for the endpoint, network, cloud and identity, AI Detection and Response (AIDR) detects and prevents direct and indirect prompt injection, jailbreaks, and model manipulation attempts.

At its core, cybersecurity is fundamentally a data problem. Fortunately, AI–and specifically Agentic AI-which takes bounded actions on users' behalf–radically empowers defenders. One of the most immediate areas Agentic AI can improve cybersecurity practices is leveraging agents to eliminate bottlenecks in the Security Operations Center (SOC). By deploying specialized agents to tackle time-intensive tasks, security teams can reclaim a speed advantage, close persistent labor and response gaps, and shift from reactive to proactive defense. Agents can analyze malware, perform certain hunt actions, prioritize exposure remediation, and more.[9]

Recommendations

- **Public and private organizations must take reasonable actions to defend themselves.** Denying cyber threat actors the ability to achieve their objectives is an important ordering principle for investments in cybersecurity capabilities. How to achieve this will continue to evolve over time in line with technological adoption and adversary techniques. Right now, enterprises should view endpoint detection and response (EDR), threat hunting, identity threat detection and response, SaaS security, and cloud security as high-leverage areas of investment to this end.

[8] In July 2017, we called on the cybersecurity community to "*bring more energy to this fight. A serious commitment from law enforcement and the security community to attempt to take down one botnet every week would be a "game changer."... These goals are ambitious relative to the status quo, but not impossible. Ultimately, focusing on such initiatives would provide a powerful organizing principle for decision makers across government and industry, going well beyond botnets and automated threats to catalyze a seismic shift in cybersecurity*." https://www.ntia.gov/files/ntia/publications/crowdstrike-20170713.pdf. Sadly, as a community we've never approached this scale.

[9] Such agents are central to a profound change that's underway now to modernize traditional SOCs for the emerging era of the Agentic SOC. A NextGen SIEM capability will enable organizations to leverage these agents by exposing them to all relevant security data and positioning them to perform workflows like threat hunting and remediation.

- **The cybersecurity community should radically increase the operational tempo of malicious infrastructure disruptions and takedowns** that are carried out by government organizations and aided by private sector support where appropriate (e.g., information sharing and operational collaboration). In some instances, private actors like IT providers or telecommunications companies can leverage legal processes or their own terms of service to disrupt operations themselves.
- **Given its stakeholder engagement functions, CISA should be central to coordinating public and private actors to this end.** This Committee can ensure that CISA[10] is properly focused and resourced to perform this mission. From an oversight perspective, you can ensure it has authorities, talent, and capabilities to maximize its impact.
- **Federal law enforcement, along with Title 10 and Title 50 entities, should work to increase deterrence.** The USG should lead holistic responses to significant adversary actions, leveraging existing authorities in parallel and with speed to deter adversaries and reduce the ROI for their attacks,

Thank you again for the opportunity to testify today, and I look forward to your questions.

###

[10] Organizations operating under Title 10 and Title 50 authorities have a somewhat more complicated resource allocation question,

Statement before the House Committee on Homeland Security

Subcommittee on Cyber and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland."

A Testimony by:

Emily Harding

Vice President,
Defense and Security
Department

Director,
Intelligence, National
Security, and
Technology Program

Center for Strategic
and International
Studies

Introduction

Chairman Ogles, Ranking Member Swalwell, distinguished Members of the subcommittee, thank you for the opportunity today to testify on this important topic. The Center for Strategic and International Studies (CSIS) does not take policy positions, so the views represented in this testimony are my own and not those of my employer.

Washington has failed to establish deterrence in the cyber domain, and our adversaries control the escalation ladder. Historically, U.S. foreign policy has rested on deterrence, with implied escalation dominance in any domain. But that foundation has failed in the context of cyber. U.S. responses to cyberattacks have been muted, and escalation dominance does not exist.

The U.S.'s offensive cyber capabilities are strong, perhaps unmatched. U.S. Cyber Command (CYBERCOM) has repeatedly proven its capability to disrupt adversary activity, when given the chance. This demonstrated skill, coupled with overall U.S. strength, makes deterrence in the cyber domain possible.

But to actually achieve deterrence, we need a mindset shift. We need to stop thinking about cyber attacks as inevitable nuisances and start seeing them for what they are: hostile action against the United States. Attacks are not always conducted by foreign States—we still need to draw a distinction between crime and hostile activity—but when they are, they should be treated as a type of warfare. China, Russia, Iran, and North Korea do not see a bright line between war and peace. Instead, they view cyber attacks as fitting on a spectrum of warfare. For them, competition with the United States is ongoing, and low-level elements of cyber warfare are not only acceptable, they are effective.

The Problem: Weak Defense and Absent Deterrence

U.S. defenses are unacceptably weak, for a set of logical reasons. The U.S. government and industry need to put considerable effort and resources toward making critical infrastructure and government systems resilient and ready for this new form of warfare. Systems must be able to fail, reset, and recover in minutes, not days, with minimal disruption to essential services.

We have a long way to go. A series of attacks in 2023 showed the severity of the gaps in stark relief. In November 2023, a designated terrorist group that is also the covert action arm of the Iranian government, the Islamic Revolutionary Guard Corps (IRGC), attacked U.S. water plants. The stated target was an Israeli company that makes software for control systems, and the attack was meant to be retaliation for the war in Gaza. While the intent was to embarrass Israel, the facts are undeniable: A terrorist group attempted to impair water delivery to civilians in the United States. Also in late 2023, the National Security Agency (NSA) and cybersecurity researchers raised renewed alarm about China's Volt Typhoon group. The attackers burrowed

into U.S. water, power, and port systems across the mainland and in Guam. These accesses could give Beijing the capability to severely disrupt daily life, particularly around the U.S. military bases that would serve as the launching pads for U.S. troops in a Pacific fight.

These two egregious violations received little attention because they were cyberattacks, and "cyber" has been shunted into a silo of what tech people do behind the scenes. It's separate, "technical," and an afterthought, not an integrated tool of modern foreign policy. This mindset is a strategic mistake. While U.S. policymakers allow these de facto silos, our adversaries are aggressively pursuing an integrated strategy. While the United States seeks to protect civilians and carefully selects offensive cyber actions, adversaries are pushing the envelope.

Attacks like Iran's and China's should be viewed as part of a dangerous new phase in cyberwarfare, one for which U.S. systems and policy are ill-prepared. To test how policymakers might respond in a massive cyberattack on U.S. territory, CSIS ran a series of wargames. The results revealed the likely disastrous confusion that would occur in a cyber-first conflict, as policymakers lack shared frameworks and a coherent view on what constitutes an act of war or a proportional response in the cyber domain. Participants shared comments like "we should use a proportional response, as soon as we figure out what a proportional response is." These exercises revealed that decision-makers do not fully understand how cyber attacks fit into traditional conceptions of the tools of foreign policy. The U.S. government has no hope of deterring, defending, and responding unless it begins to integrate cyber offense and defense into its own national security strategy. In the Trump Administration's recently released National Security Strategy, its explicit mention of "offensive cyber operations" as part of a comprehensive U.S. government response capability is a positive development.

How to Fix It: Recommendations

The U.S. government needs to establish a new framework for conceptualizing and responding to these kinds of attacks. To address this urgent need, CSIS created a Playbook for Winning the Cyber War, which lays out how to shift the mindset, plus actionable steps for building the larger capacity to fight this modern form of warfare. The steps are summarized below: creating a new declaratory policy, rethinking U.S. internal policies, building an international response, and operationalizing the shift.

Announce the Shift: A New Declaratory Policy on Cyber Warfare

The first part of a mindset shift is for the U.S. government to **establish a new declaratory policy** with the following key points:

- **Cyberattacks are attacks.** If they imperil life, health, or safety, and particularly if they threaten critical infrastructure in a way that could create a mass casualty event, the U.S. government will treat them as they would any other attack on civilians.

- **The United States can and will use all elements of state power** to effectively defend the homeland against any threat, in any domain. Further, the U.S. prides itself on protecting innocent civilians, not targeting them, so it refuses to target civilian critical infrastructure. Therefore, a proportional response to a cyberattack on our critical infrastructure would be severe and likely include economic or military measures.
- The United States will assume any cyberattack on critical infrastructure has a destructive intent and respond accordingly.

Internalize the Shift for US Decisionmakers

Redefine proportionality and escalation to include the big picture. Policymakers' view of proportionality must expand beyond the most recent incident and consider the aggregate costs of a pattern of attacks, the long-term economic and security consequences of those attacks, and the message sent by inaction. A new policy, which could be called "cyber first–cyber optional," must begin with explicit principles that the United States is redefining proportionality in the cyber domain, bolstering defense, and putting adversaries on notice that in the future the United States will retaliate for the overall pattern of behavior, not any one attack in isolation, and will use all tools at its disposal. A cyber response to a cyber attack is an option, but far from the only option.

Take the Shift International

Define international norms of behavior to establish a clear baseline for future action. This is a worthwhile exercise, even if many States are likely to ignore those norms. Defining the norms lays the groundwork for deterrence, because it reduces uncertainty around action when those norms are violated. Not just the statement, but the demonstration of will is critical to deterrence. A strong U.S. and allied response to the first cyberattack after the declaratory policy goes into place will help set a new tone.

Operationalize the Shift

Evolve offensive operations to operate as a strategic whole. Cyber policy plays a late, minor supporting role to the main characters in foreign policy. The needed evolution, then, depends on two actions: (1) sliding risk tolerance far higher, freeing operators to do more as the opportunity arises, and (2) shifting planning far to the left on the timeline, incorporating cyber tools in the early-stage policy planning process. Then, policymakers will be ready to run a new, more robust playbook to win the cyber war.

First, adjust risk tolerance. A shift toward a higher risk tolerance for rapid action is essential for a more flexible, aggressive approach. Cyber offense must combine long-term planned campaigns and instant opportunism. A large campaign is essential to create a coherent long-term approach, but within that campaign, operators must be prepared to seize upon a vulnerability in the rare moment it appears. Ideally policymakers would flip the risk calculus: The default answer

to a proposed operation should be "yes," and a naysayer must prove it is too risky instead of asking the operators to prove the operation is safe.

Second, collaborate early. Cyber, in its relative newness, often gets relegated to a last-minute add-on to an operational plan instead of playing an integrated role in a larger campaign. This approach can allow cyber activity to contribute somewhat, but only on the margins. Instead, planners should incorporate cyber operators into early-stage planning, particularly for contingency planning against a peer competitor. If developed early enough, cyber tools can distract and weaken an adversary, serving as a force multiplier for military and diplomatic action. Being ready to capitalize on lucky opportunities takes months of research, planning, and prepositioning. If cyber tools are to be available in moments of acute need, operators need lead time to plan.

This evolved model could be imagined as an octopus. Offensive cyber tools, at their best, are flexible, inventive, and opportunistic, akin to how an octopus hunts in the wild. Cyber offense must combine long-term planned campaigns and instant opportunism—like an octopus's central brain and tentacles. An octopus camouflages itself perfectly, uses its tentacles to explore nooks and crannies, and squeezes into impossibly small corners to wait for its prey. Further, each tentacle acts independently but also as part of a whole. The central nervous system guides the effort, but a brain in each tentacle manages the search. An octopus model for offensive cyber operations might include strategic guidance from the NSC; interagency campaign planning; a forward-leaning approach to exploration and opportunism; and additional delegated responsibility to NSA, CIA, and CYBERCOM for execution of low- and moderate-risk missions.

With these pieces in place, run the playbook. CSIS's report lays out these steps in detail, but the main point is this: Be bold. Match creative policy responses to the pain points of the particular attacker. Demonstrate that the United States will view a cyberattack that causes damage as just as serious as a kinetic attack.

Recommendations for Congress

The following Congressional actions can bolster cyber offensive capability, bolster domestic defense, and help create much-needed deterrence:

- Create and fund a new Cyber Force: The cyber domain needs its own service, heavily weighted toward reserve forces, to recruit and retain the best cyber talent from the private sector.
- Fund cybersecurity: Congress should consider funding much-needed capital upgrades in government networks, allow more flexible spending for cybersecurity improvements, and require improved reporting and greater accountability for weak cyber defense inside government. They should also consider creating a combination of funding streams (carrots) and consequences (sticks) for critical infrastructure providers to significantly improve their resilience against attacks.

- Protect industry cyber fighters: Treat the private sector as real partners. Put in place protections for cyber operators who act in conjunction with the U.S. government, as so many from the private sector did in Ukraine.

Conclusion

A dramatic change is needed in the cyber domain. Washington urgently needs to integrate cyber into its broader foreign policy toolkit and determine how cyber activity aligns with larger foreign policy actions, including deterrence, proportional response, and international norms. In other words, the United States needs a new playbook to respond to increasingly disruptive and aggressive cyberattacks. For more, see CSIS's *A Playbook for Winning the Cyber War*.

JOE LIN WRITTEN TESTIMONY

Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

"Defense through Offense: Examining U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland"

Tuesday, January 13, 2026

Chairman, Ranking Member, and Members of the Committee,

Thank you for the opportunity to speak before you today. My name is Joseph Lin. I am the CEO of Twenty, the first U.S. venture-backed cyber warfare start-up, building industrial-scale offensive cyber capabilities for the United States and its allies. I've spent my career working alongside the Intelligence Community, the Department of War, and civilian agencies defending American networks.

My co-founders and I founded this company for a simple reason: America is under sustained cyber attack, and our adversaries have learned—correctly—that those attacks rarely produce consequences. We decided to change that—by making our adversaries think twice before they attack us.

For too long, Washington has treated offensive cyber operations as inherently escalatory — as if responding to a cyber intrusion carried the same risk as nuclear war. The result is a dangerous pattern: we absorb attack after attack, issue warnings about "norms," and add a modest sanction or two. Meanwhile, the People's Republic of China (PRC), Russia, Iran, and North Korea continue to infiltrate our critical infrastructure, steal our intellectual property, and pre-position malware inside our civilian systems — all with increasing confidence that there will be no real cost.

That restraint was meant to prevent escalation. In practice, it has invited it.

The following is a small fraction of the persistent and escalating campaign of cyber aggression directed against the United States.

We have watched as PRC-linked actors conducted the Salt Typhoon campaign, making deep, strategic infiltrations into multiple major American telecommunications providers, including AT&T, Verizon, and T-Mobile.

We have witnessed the systematic theft of our citizens' most private data:

- The compromise of Anthem impacted 79 million records—including Social Security numbers and medical IDs.

- We have seen the mass exfiltration of personal data from Marriott affect 383 million guests, including passport numbers.
- We have seen 145 million Americans—nearly half the country—have their financial identities stolen in the Equifax breach, an act for which members of the Chinese Military were directly indicted.
- We have seen 22 million records exfiltrated from the Office of Personnel Management, including the highly sensitive SF-86 security clearance files of our federal workforce. It included the Social Security numbers, fingerprints, and the most intimate background details of current, former, and prospective federal employees, contractors, and their families. By harvesting this data, the PRC has gained a permanent counterintelligence roadmap to the people who operate, protect, and lead this country.

Additionally, PRC actors have moved beyond espionage and begun embedding themselves within our critical infrastructure.

Through the campaign known as Volt Typhoon, PRC-linked actors have burrowed into the networks of U.S. water, power, and transit systems. According to public government reporting, this activity reflects deliberate pre-positioning to hold hostage our American cities and communities, and enable disruption during a future crisis or conflict.

The PRC is not alone. The 2014 Sony Pictures hack—conducted by North Korean actors—was not about theft alone. It was designed to destroy systems, disrupt operations, and impose real economic damage on a U.S. company.

These are no longer potential risks.

Our adversaries have learned that the marginal cost of doing more is low. Every time we respond to aggression with speeches instead of real consequences, we send a clear signal: keep climbing. Over time, that becomes a perverse incentive — one that rewards exactly the behavior we want to stop.

The cyber domain doesn't behave like the Cold War's nuclear world. Escalation is not automatic — which means policymakers have more room to act than their instincts suggest. We don't have to choose between doing nothing and doing something reckless. We can act proportionally, preemptively, and persistently.

Last year, National Cyber Director Sean Cairncross was correct in saying that the US needs to "shift the burden of risk in cyberspace from Americans to them." Director Cairncross recognizes that deterrence in cyberspace requires the credible, routine use of offensive power — not as a last resort, but as a standing expectation. Our adversaries are not deterred by words; they are deterred by disruption.

And the most effective time to disrupt an adversary is before their campaign becomes a headline. Preemptive operations — when executed responsibly — can deny access, degrade infrastructure, and raise the attacker's cost curve. They force our enemies to rebuild, defend, and think twice.

In the physical world, we would never allow a terrorist to walk across our borders, establish a terrorist cell in plain sight, and wait to stop them only at the moment they reach for the detonator. We don't wait for the trigger to be pulled or the button to be pressed on a bomb. We stop them well before they ever reach their target. Afterwards, our military, intelligence community, and law enforcement are praised for their ability to identify hostile infrastructure being built for the purpose of attacking America.

Cyberspace should be no different. We currently possess the technical ability to see the digital infrastructure of our enemies being constructed in the shadows of our networks. We can see the networking established with the intention to paralyze us. Yet, under our current passive doctrine, we are forced to watch and wait.

We need a policy of deterrence where we disrupt the threat at its origin, not at our doorstep. We can leverage the innovation of the private sector to dismantle these threats before they can be activated. If we can foresee an attack aimed at an American city or town, a Fortune 500 company or a federal agency, a state or local municipality, our duty is clear: we have the moral and national security obligation to neutralize the threat.

At Twenty, we partner closely with the United States Government to develop and deploy these capabilities at scale. We're helping to deliver exactly what deterrence now requires: speed, agility, and credible offensive power.

But this is not just about technology — it's about mindset. For years, we substituted process for power. We talked about responsible behavior, issued indictments that foreign operatives will never face, and redrew red lines every time they were crossed. That approach has failed not because America lacks cyber talent, but because we have been paralyzed by outdated theories of escalation.

To compete, we must build a new habit—responding. Every serious campaign against the United States must produce real, visible consequences.

Congress has a critical role to play by demanding measurable accountability. On a classified basis, Congress should require answers to the following questions: How quickly and how often were preemptive or proactive offensive cyber actions authorized to disrupt, deny, or degrade adversary operations? Did those actions reduce adversary persistence? And were hostile campaigns forced to degrade or rebuild?

These are the questions that should define cyber deterrence in the 21st century.

Technology will play a decisive role in this transformation — especially Artificial Intelligence. AI-enabled systems are already reshaping cyber operations, from accelerating target analysis to automating detection of vulnerabilities. At Twenty, we are developing AI-driven cyber tools that can operate securely within classified environments, multiply human capability by orders of magnitude, and do so responsibly, with human oversight.

Last year, Congress authorized one billion dollars for offensive cyber programs in H.R. 1. This was an important step, but only a down payment. We cannot treat it as a box checked. These funds must go toward future-focused technology — not legacy systems — and AI must be a central part of that investment. And, Congress should condition future offensive cyber funding on demonstrable improvements in speed, scale, and mission impact—favoring systems built for rapid, persistent cyber operations, not legacy platforms designed for episodic, one-off missions.

Ultimately, no single entity — not government, not industry — can meet this challenge alone. Our adversaries coordinate across government and private lines. We must do the same. The White House is right to emphasize public-private collaboration as a cornerstone of cyber deterrence. The United States has the talent, the innovation, and the moral clarity to lead in this new era — but leadership requires urgency, and it requires partnership.

At Twenty, we are proud to help make that possible — ensuring that America's cyber capabilities remain powerful, disciplined, and aligned with democratic values.

Thank you for the opportunity to testify. I look forward to your questions.