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*.