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.