

DEFENSE THROUGH OFFENSE: EXAMINING U.S.
CYBER CAPABILITIES TO DETER AND DISRUPT
MALIGN FOREIGN ACTIVITY TARGETING THE
HOMELAND

HEARING
BEFORE THE
SUBCOMMITTEE ON
CYBERSECURITY AND INFRASTRUCTURE
PROTECTION
OF THE
COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED NINETEENTH CONGRESS
SECOND SESSION
JANUARY 13, 2026
Serial No. 119-34

Printed for the use of the Committee on Homeland Security



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

63-558 PDF

WASHINGTON : 2026

COMMITTEE ON HOMELAND SECURITY

ANDREW R. GARBARINO, New York, *Chairman*

MICHAEL T. MCCAUL, Texas, <i>Vice Chair</i>	BENNIE G. THOMPSON, Mississippi, <i>Ranking Member</i>
MICHAEL GUEST, Mississippi	ERIC SWALWELL, California
CARLOS A. GIMENEZ, Florida	J. LUIS CORREA, California
AUGUST PFLUGER, Texas	SHRI THANEDAR, Michigan
TONY GONZALES, Texas	SETH MAGAZINER, Rhode Island
MORGAN LUTTRELL, Texas	DANIEL S. GOLDMAN, New York
DALE W. STRONG, Alabama	DELIA C. RAMIREZ, Illinois
JOSH BRECHEEN, Oklahoma	TIMOTHY M. KENNEDY, New York
ELIJAH CRANE, Arizona	LAMONICA MCIVER, New Jersey
ANDREW OGLES, Tennessee	JULIE JOHNSON, Texas, <i>Vice Ranking Member</i>
SHERI BIGGS, South Carolina	PABLO JOSÉ HERNÁNDEZ, Puerto Rico
GABE EVANS, Colorado	NELLIE POU, New Jersey
RYAN MACKENZIE, Pennsylvania	JAMES R. WALKINSHAW, Virginia
BRAD KNOTT, North Carolina	TROY A. CARTER, Louisiana
VINCE FONG, California	AL GREEN, Texas
MATT VAN EPPS, Tennessee	
VACANT	

KEIGHLE JOYCE, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

ANDREW OGLES, Tennessee, *Chairman*

CARLOS A. GIMENEZ, Florida	ERIC SWALWELL, California, <i>Ranking Member</i>
MORGAN LUTTRELL, Texas	SETH MAGAZINER, Rhode Island
RYAN MACKENZIE, Pennsylvania	LAMONICA MCIVER, New Jersey
VINCE FONG, California	JAMES R. WALKINSHAW, Virginia
ANDREW R. GARBARINO, New York (<i>ex officio</i>)	BENNIE G. THOMPSON, Mississippi (<i>ex officio</i>)

ROLAND HERNANDEZ, *Subcommittee Staff Director*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

CONTENTS

	Page
STATEMENTS	
The Honorable Andrew Ogles, a Representative in Congress From the State of Tennessee, and Chairman, Subcommittee on Cybersecurity and Infrastructure Protection:	
Oral Statement	1
Prepared Statement	3
The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Oral Statement	4
Prepared Statement	5
WITNESSES	
Mr. Joe Lin, Co-Founder and Chief Executive Officer, Twenty Technologies, Inc.:	
Oral Statement	7
Prepared Statement	8
Ms. Emily Harding, Vice President, Defense and Security Department, Center for Strategic and International Studies:	
Oral Statement	10
Prepared Statement	12
Mr. Frank Cilluffo, Director, McCrary Institute for Cyber and Critical Infrastructure Security, Auburn University:	
Oral Statement	15
Prepared Statement	17
Mr. Drew Bagley, Chief Privacy Officer, CrowdStrike:	
Oral Statement	19
Prepared Statement	21

DEFENSE THROUGH OFFENSE: EXAMINING U.S. CYBER CAPABILITIES TO DETER AND DISRUPT MALIGN FOREIGN ACTIVITY TAR- GETING THE HOMELAND

Tuesday, January 13, 2026

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY AND
INFRASTRUCTURE PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:02 a.m., in room 310, Cannon House Office Building, Hon. Andy Ogles [Chairman of the subcommittee] presiding.

Present: Representatives Ogles, Gimenez, Luttrell, Fong, Swalwell, Magaziner, McIver, and Walkinshaw.

Also present: Representatives Thompson, and Garbarino.

Mr. OGLES. The Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of today's hearing is to examine the current state of U.S. capabilities or how those capabilities are used to deter, disrupt, and impose real cost on foreign adversaries that target the homeland and our Nation's critical infrastructure. The hearing will also assess the legal authorities that govern offensive cyber operations across the Federal Government and examine the evolving role of the private sector as the U.S. Government considers whether and under what circumstances private entities may be authorized to support or conduct offensive and disruptive cyber activity.

I now recognize myself for an opening statement.

Today, the subcommittee is meeting to examine a reality that the United States can no longer afford to avoid, namely that deterrence in cyber space does not exist without credible, lawful, and operational offensive cyber capabilities. Defense alone is not sufficient. Resilience alone is not sufficient. Public attribution alone is not sufficient.

For more than a decade, the United States has invested heavily in cyber defense and information sharing and resilience. Those investments are necessary and they have improved our ability to withstand attacks, but they have not altered adversarial behavior. Malign cyber actors continue to penetrate American networks, steal sensitive data, surveil communications, and position themselves in-

side critical infrastructure with little fear of meaningful consequence.

That reality was reinforced again just days ago, when public reporting revealed that a Chinese state-sponsored cyber actor known as Salt Typhoon compromised email systems used by staff supporting several Congressional committees. This incident was the latest operation in a sustained campaign conducted by a broader group of Chinese cyber actors commonly referred to as the Typhoon Cluster. These actors are not criminals acting for profit. They are instruments of state power, and that needs to be underscored.

Their operations are deliberate, persistent, and strategic in nature. They are designed to extract intelligence, pre-position access, and shape the battlefield long before a crisis or conflict emerges. I am going to say that again. Pre-position access and shape the battlefield long before a crisis or conflict emerges. They target not only the Executive branch and private industry, but now, once again, the Legislative branch itself.

The question before this subcommittee is not whether these threats exist. That is no longer in dispute. The question is why they continue and what it will take to change the cost-benefit calculation for adversaries who believe they can operate against the United States with impunity.

Currently, authorities for offensive cyber operations are dispersed across the Department of War, the intelligence community, law enforcement, while civilian agencies like CISA play critical roles in defense, response, and resilience. Existing policy frameworks were developed for an earlier phase of the cyber threat environment, one that did not fully anticipate today's scale, speed, and persistence of state-sponsored activity. Again, the speed and the scale of the battlefield has changed. They are also not designed for a world in which the vast majority of digital infrastructure targeted by adversaries is owned and operated by the private sector.

The reality is forcing a broader reassessment across the Federal Government. The Trump administration has signaled its intent to pursue a more proactive and assertive cyber posture, one that emphasizes disrupting adversary capabilities before harm occurs, resetting adversarial risk calculations, and exploring new ways to integrate private-sector expertise into national cyber efforts. This reflects an important recognition. The private sector is not merely a victim in cyber space. American cybersecurity companies, cloud providers, telecommunications firms, and emerging technology start-ups are often the first to detect malicious activity, the first to analyze adversarial tradecraft, and the first to develop tools capable of disrupting hostile infrastructure. In many cases, they already possess visibility and technical insights that rivals or exceeds that of the Federal Government.

The challenge is that much of this activity exists in legal and policy gray space. Companies face uncertainty about liability, retaliation, and regulatory risk. Government agencies face constraints on how they can partner, share information, and act with speed. Adversaries exploit these seams, operating continuously below the threshold of armed conflict while benefiting from ambiguity and restraint.

Today, our witnesses will help us assess how offensive cyber capabilities can be responsibly integrated into a modern homeland security framework. I appreciate our witnesses for being here and I look forward to their testimony and the discussion ahead. Again, thank you all for being here.

[The statement of Chairman Ogles follows:]

STATEMENT OF CHAIRMAN ANDREW OGLES

JANUARY 13, 2026

Today, the subcommittee is meeting to examine a reality that the United States can no longer afford to avoid, namely that deterrence in cyber space does not exist without credible, lawful, and operational offensive cyber capabilities. Defense alone is not sufficient. Resilience alone is not sufficient. Public attribution alone is not sufficient.

For more than a decade, the United States has invested heavily in cyber defense, information sharing, and resilience. Those investments are necessary and they have improved our ability to withstand attacks. But they have not altered adversary behavior. Malign cyber actors continue to penetrate American networks, steal sensitive data, surveil communications, and position themselves inside critical infrastructure with little fear of meaningful consequence.

That reality was reinforced again just days ago, when public reporting revealed that a Chinese state-sponsored cyber actor known as Salt Typhoon compromised email systems used by staff supporting several Congressional committees. This incident was the latest operation in a sustained campaign conducted by a broader group of Chinese cyber actors commonly referred to as the Typhoon cluster.

These actors are not criminals acting for profit. They are instruments of state power. Their operations are deliberate, persistent, and strategic in nature. They are designed to extract intelligence, pre-position access, and shape the battlefield long before a crisis or conflict emerges. They target not only the Executive branch and private industry, but now once again the Legislative branch itself.

The question before this subcommittee is not whether these threats exist. That is no longer in dispute. The question is why they continue, and what it will take to change the cost-benefit calculation for adversaries who believe they can operate against the United States with impunity.

Currently, authorities for offensive cyber operations are dispersed across the Department of War, the intelligence community, and law enforcement, while civilian agencies like CISA play critical roles in defense, response, and resilience. Existing policy frameworks were developed for an earlier phase of the cyber threat environment, one that did not fully anticipate today's scale, speed, and persistence of state-sponsored cyber activity.

They were also not designed for a world in which the vast majority of digital infrastructure targeted by adversaries is owned and operated by the private sector.

That reality is forcing a broader reassessment across the Federal Government. The Trump administration has signaled its intent to pursue a more proactive and assertive cyber posture, one that emphasizes disrupting adversary capabilities before harm occurs, resetting adversary risk calculations, and exploring new ways to integrate private-sector expertise into national cyber efforts.

This reflects an important recognition. The private sector is not merely a victim in cyber space. American cybersecurity companies, cloud providers, telecommunications firms, and emerging technology start-ups are often the first to detect malicious activity, the first to analyze adversary tradecraft, and the first to develop tools capable of disrupting hostile infrastructure. In many cases, they already possess visibility and technical insight that rivals or exceeds that of the Federal Government.

The challenge is that much of this activity exists in legal and policy gray space. Companies face uncertainty about liability, retaliation, and regulatory risk. Government agencies face constraints on how they can partner, share information, and act with speed. Adversaries exploit these seams, operating continuously below the threshold of armed conflict while benefiting from ambiguity and restraint.

Today, our witnesses will help us assess how offensive cyber capabilities can be responsibly integrated into a modern homeland security framework.

I appreciate our witnesses for being here, and I look forward to their testimony and the discussion ahead.

Thank you.

Mr. OGLES. I now recognize the Ranking Member, the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you, Mr. Chairman. Good morning. I appreciate the opportunity to discuss opportunities to disrupt and deter malicious cyber activities on domestic networks and impose cost on our adversaries. I thank the witnesses for participating.

Before I begin, however, I would like to send my deepest condolences to the family of Renee Good, particularly her partner and 6-year-old child, who is now without a mother. From everything I have seen, Ms. Good was attempting to de-escalate and leave the situation and there was no reason to take her life. I support a full investigation of this shooting and justice on her behalf.

Turning to the issue at hand, over the course of the past year, there have been increased discussions about whether the United States is using its formidable offensive cyber capabilities as effectively as it could be to deter and disrupt cyber attacks. United States' offensive cyber capability is second to none, but with that awesome power comes awesome responsibility. As we consider whether and how to deploy offensive cyber tools differently, we must bear three points in mind.

First, cyber offense is no substitute for defense and resilience. We will have to continue investing in those key capabilities.

Second, cyber offense is one tool among many, including sanctions and other diplomatic levers, that the United States can use to shape adversary behavior. The tool of—combination of tools we should align with our mission objectives.

Finally, any significant change to our approach to the use of offensive cyber operations could shift global norms, and we must consult our allies.

As a committee responsible for overseeing the Cybersecurity and Infrastructure Security Agency, referred to as CISA, I am concerned that we are putting the cart before the horse with a hearing on offensive cyber activity when we have not had a hearing on why the agency has lost one-third of its work force over the last year. CISA is an agency responsible for helping utilities, water treatment facilities, pipelines, and other critical infrastructure entities keeping Volt Typhoon and other adversaries off our network. But ever since last January, the Trump administration harassed key CISA personnel into leaving their jobs, including the individuals responsible for the Secure-by-Design Program, the Pre-Ransomware Notification Initiative, and individuals who work directly with critical infrastructure operators on security issues. We ought to be cautious about pursuing an approach involving the use of offensive cyber tools that could result in retaliation or escalation if we are not in a position to help defend U.S. networks.

Moreover, we must bear in mind that offensive tools are one of many tools at our disposal to shape behavior in cyber space, and we need to use them all more effectively and more deliberately. I understand that plans to impose sanctions on China's Ministry of State Security for its Salt Typhoon campaign was put on hold last year as the President negotiated a trade truce with the country. Our use of sanctions and other diplomatic tools to deter and impose cost on our adversaries would be more effective if the President did not start unnecessary trade wars. Relatedly, we should be clear-

eyed about what our objectives are and how the use of offensive cyber tools align with our objectives.

Finally, any change in our approach to the use of offensive cyber tools that would shift current norms must be done in consultation with our allies. We cannot afford to distance ourselves from our security partners more than this administration already has.

Having said that, I agree there are opportunities to increase pressure and impose higher costs on adversaries for unacceptable behavior in cyber space. We should consider whether there are many—where there are ways to more aggressively disrupt adversary infrastructure and deny them the benefits of success. Additionally, while offensive cyber activities by and large is a Government function, there may be new ways for the private sector to support Government efforts in this space in a manner consistent with the law.

I look forward to discussing these issues, and I yield back the balance of my time.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JANUARY 13, 2026

I appreciate the opportunity to discuss opportunities to disrupt and deter malicious cyber activities on domestic networks and impose costs on our adversaries, and I thank the witnesses for participating.

Before I begin, however, I would like to send my deepest condolences to the family of Renee Good, particularly her partner and 6-year-old child, who is now without a mother. From everything I've seen, Ms. Good was attempting to de-escalate and leave the situation, and there was no reason to take her life. I support a full investigation of this shooting and justice on her behalf.

Turning to the issue at hand, over the course of the past year, there has been increased discussion about whether the United States is using its formidable offensive cyber capabilities as effectively as it could be to deter and disrupt cyber attacks. The United States' offensive cyber capability is second-to-none—but with that awesome power comes awesome responsibility. As we consider whether and how to deploy offensive cyber tools differently, we must bear three points in mind:

First, cyber offense is no substitute for defense and resilience. We will have to continue investing in those key capabilities. Second, cyber offense is one tool among many—including sanctions and other diplomatic levers—that the United States can use to shape adversary behavior. The tool—or combinations of tools—we use should align with our mission objectives. Finally, any significant change to our approach to the use of offensive cyber operations could shift global norms, and we must consult our allies.

As the committee responsible for overseeing the Cybersecurity and Infrastructure Security Agency (CISA), I am concerned that we are putting the cart before the horse with a hearing on offensive cyber activity when we have not yet had a hearing on why the agency has lost one-third of its workforce over the past year. CISA is the agency responsible for helping utilities, water treatment facilities, pipelines, and other critical infrastructure entities keep Volt Typhoon and other adversaries off their networks.

But ever since last January, the Trump administration harassed key CISA personnel into leaving their jobs, including the individuals responsible for the Secure-by-Design program, the Pre-Ransomware Notification Initiative, and individuals who worked directly with critical infrastructure operators on security issues.

We ought to be cautious about pursuing an approach involving the use of offensive cyber tools that could result in retaliation or escalation if we are not in a position to help defend U.S. networks.

Moreover, we must bear in mind that offensive tools are one of many tools at our disposal to shape behavior in cyber space—and we need to use them all more effectively and more deliberately. I understand that plans to impose sanctions on China's Ministry of State Security for its Salt Typhoon campaign were put on hold last year as the President negotiated a trade "truce" with the country.

Our use of sanctions and other diplomatic tools to deter and impose costs on our adversaries would be more effective if our President did not start unnecessary trade wars. Relatedly, we should be clear-eyed about what our objectives are and how the use of offensive cyber tools aligns with those objectives.

Finally, any change in our approach to the use of offensive cyber tools that would shift current norms must be done in consultation with our allies. We cannot afford to distance ourselves from our security partners more than this administration already has. Having said all that, I agree there are opportunities to increase pressure and impose higher costs on adversaries for unacceptable behavior in cyber space.

We should consider whether there are ways to more aggressively disrupt adversary infrastructure and deny them the benefits of success. Additionally, while offensive cyber activity is a Government function, there may be new ways for the private sector to support Government efforts in this space, in a manner consistent with the law.

Mr. OGLES. Thank you, Ranking Member Thompson. Other Members of the committee are reminded that opening statements may be submitted for the record.

I am pleased to have a distinguished panel of witnesses before us today on this important topic. Pursuant to committee rule VIII(C), I ask that our witnesses please rise and raise their right hands.

[Witnesses sworn.]

Mr. OGLES. Let the record reflect that the witnesses have answered in the affirmative. Thank you and please be seated.

I would like to formally introduce our witnesses. Mr. Joe Lin currently serves as co-founder and CEO of Twenty Technologies, a cybersecurity company that develops AI-enabled capabilities to help Government and national security partners detect, disrupt, and counter sophisticated cyber threats. In addition to his current role, he is a commissioner on the Center for Strategic and International Studies Commission on Cyber Force Generation. Prior to his roles at Twenty, Mr. Lin served as the vice president of product management at Palo Alto Networks, where he founded and led the National Security Division. A former U.S. Navy Reserve officer, Mr. Lin has spent over a decade defending U.S. military, Government, and critical infrastructure networks. Thank you, Mr. Lin.

Ms. Emily Harding currently serves as vice president of the Defense and Security Department and director of the Intelligence, National Security, and Technology Program at the Center for Strategic and International Studies. That is a mouthful. In these roles, she provides expert knowledge and intellectual leadership on issues shaping the future of intelligence work and national security. Prior to CSIS, Ms. Harding served as the deputy staff director on the Senate Select Committee on Intelligence, led analytic programs at the CIA, and contributed to the first Office of the Director of National Intelligence-led Presidential transition.

Mr. Frank Cilluffo serves as the director of Critical Infrastructure Security at Auburn University. He was a member of the U.S. Cyber Solarium Commission and served as special assistant to the President in George W. Bush's administration in the newly-created White House Office of Homeland Security. Following this role, he joined George Washington University where he established the Center for Cyber and Homeland Security. His previous experience also includes senior policy positions at the Center for Strategic and International Studies. Thank you, Ms. Harding—Mr. Cilluffo.

Mr. Drew Bagley currently serves as the chief privacy officer at CrowdStrike, where he is responsible for leading the company's global data protection initiatives, privacy strategy, and policy engagement. Mr. Bagley previously worked in the Federal Bureau of Investigation's Office of the General Counsel. Has served as an advisor to Government and nonprofit groups, including the Cybersecurity Infrastructure Security Agency's Joint Cyber Defensive Collaborative at the U.S. Department of State and Europol. In addition to his corporate leadership, Mr. Bagley serves on the faculty of American University where he teaches cyber law and privacy.

I want to thank each of our distinguished witnesses for being here today. I now recognize Mr. Lin for 5 minutes to summarize his opening.

**STATEMENT OF JOE LIN, CO-FOUNDER AND CHIEF
EXECUTIVE OFFICER, TWENTY TECHNOLOGIES, INC.**

Mr. LIN. Chairman, Ranking Member, Members of the subcommittee, thank you for the opportunity to testify today. My name is Joe Lin. I'm the co-founder and CEO of Twenty Technologies, where we build industrial-scale cyber warfare capabilities for the United States.

I want to be direct. The United States is not postured to deter or defeat its adversaries in cyber space. Our adversaries, most notably the People's Republic of China, are running persistent, large-scale cyber campaigns against U.S. critical infrastructure, telecommunications, the defense industrial base, and Government networks. These are not episodic breaches. These are not just thefts of intellectual property. They are continuous, increasingly automated shaping operations designed to hold our society at risk at peacetime and to pre-position for conflict. These campaigns have been effective. They have imposed real and growing costs on the United States.

By contrast, our response is unnecessarily constrained, particularly in the use of offensive cyber. This restraint has not prevented escalation, it has encouraged it. When adversaries escalate and face little or no cost, they learn that it works. Over time, that becomes an incentive to push further. In effect, we have created a one-way dynamic. They escalate and we absorb. Because we absorb, they keep escalating. Yet the U.S. Government continues to treat offensive cyber as a bespoke capability, slow to generate, difficult to scale, and constrained by processes built for a different era. We rely on small numbers of elite teams executing one-off operations while our adversaries operate at machine speed across hundreds or thousands of targets. That mismatch is the core problem.

Deterrence in cyber space does not come from symbolic gestures or isolated tactical wins. It comes from the demonstrated ability to impose sustained asymmetric cost at scale to make adversary campaigns fail repeatedly and faster than they can adapt. This is not just a talent problem, this is a structural one. Our cyber forces are asked to confront an industrial scale threat with bespoke tools and processes. We have not built cyber capabilities for sustained campaigns, operational tempo, or mass effects. Cyber space is now a primary domain of conflict where speed, scale, and persistence de-

termine real-world outcomes. Offensive cyber must therefore be treated as a core instrument of national power, and that requires three shifts.

First, we must industrialize offensive cyber capabilities. Elite operator tradecraft must be turned into software, codified, testable, repeatable systems that execute under human authorization at machine speed. This is not about removing humans from the loop. It is about leverage. One operator should be able to direct efforts across hundreds of targets, not one.

Second, we must align authorities, acquisition, and operational concepts to sustained campaigns, not single operations. Our adversaries are persistent. We need capabilities that are continuously operating, adapting, and imposing friction, built as operational software, not legacy Government programs designed for peacetime procurement.

Third, we must be honest about the role of offense in defense. Critical infrastructure security will not be solved through patching alone. Against persistent state-directed actors, defensive measures are insufficient. Deterrence requires credible offensive cyber operations that disrupt and impose costs upstream. This may be uncomfortable culturally, but unavoidable strategically.

Effective offensive cyber is not reckless. It is disciplined, tested, authorized, and aligned with Government policy. In fact, the absence of scalable, well-engineered offensive capability increases risk by ceding initiative to our adversaries and forcing reactive, crisis-driven responses.

The United States has faced industrial-scale threats before. Each time we built industrial-scale responses. Cyber is no different except that time is not on our side. The campaigns under way today are shaping the battle space for tomorrow. Every delay compounds the problem. This subcommittee has a critical role to play. Clarifying mission ownership, enabling acquisition pathways for commercial offensive cyber capabilities, and treating offensive cyber operations as a decisive element of homeland security, not a niche activity. If we want deterrence, we must build the capabilities that make deterrence real.

Thank you and I look forward to your questions.
[The prepared statement of Mr. Lin follows:]

PREPARED STATEMENT OF JOE LIN

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 crit-

ical 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 road map 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 policy makers 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 United States needs to “shift the burden of risk in cyber space from Americans to them.” Director Cairncross recognizes that deterrence in cyber space 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.

Cyber space 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 U.S. 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 \$1 billion 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.

Mr. OGLES. Thank you, Mr. Lin. I agree, the best defense is an aggressive offense.

I now recognize Ms. Harding for 5 minutes to summarize her opening statement.

STATEMENT OF EMILY HARDING, VICE PRESIDENT, DEFENSE AND SECURITY DEPARTMENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Ms. HARDING. Thank you for this opportunity. I suspect I'm going to find myself in fierce agreement with most of my panelists here, but I'll try to add a little bit. First I want to walk a bit through the problem and then talk about the war games that we ran to fully diagnose that problem, and then a minute on how to fix it.

So the problem. Washington has failed to establish deterrence in the cyber domain and our adversaries right now 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 cyber attacks have been muted. Escalation dominance does not exist.

To actually achieve this deterrence, we need a mindset shift. We need to stop thinking about cyber attacks as inevitable nuisances and start seeing them for what they really are: hostile actions against the United States. 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 on-going. Low-level elements of cyber warfare are not only acceptable, they're effective.

In 2023, both Iran and China pushed the boundaries with attacks on critical infrastructure. In November 2023, the Islamic Revolutionary Guard Corps of Iran attacked U.S. water plants. 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, NSA and cybersecurity researchers raised renewed alarm about China's Volt Typhoon group. The attackers burrowed into U.S. water, power, port systems in the mainland and on Guam. These accesses could give Beijing the capability to disrupt daily life. This was the pre-positioning you were talking about in your opening statement, Mr. Chairman, particularly around U.S. military bases that would serve as launching pads for U.S. troops in a Pacific fight.

So let's talk a little bit about the war games we use to diagnose this problem fully. This is a dangerous new phase in cyber warfare. We suspected that U.S. policy makers had not fully wrapped their heads around what it means. So we pulled together some senior folks who had served in many previous administrations to walk them through these scenarios. One scenario, an adversary conducted an attack on critical infrastructure in the homeland where a dam malfunctioned and hundreds died. Other scenarios were more complex. We had attacks on water systems leading to sickness. We had attacks on power plants leading to deaths at hospitals and from exposure to cold.

These games revealed a stark conclusion. Our participants were confused, spinning their wheels. They had comments like, well, we should use a proportional response as soon as we figure out what a proportional response is. These are very smart people who have served at high levels of Government. This is just a hard problem they were trying to grapple with. They lack a shared framework and a coherent viewpoint on what constitutes an act of war and a proportional response in the cyber domain. In other words, while our adversaries have fully incorporated cyber into their foreign policy playbook, we are still struggling to understand what cyber is and what it should do.

So how do we fix it? The U.S. Government needs to establish a new framework for conceptualizing and responding to cyber attacks. To address this need, we wrote a recent tome of a project called "A Playbook for Winning the Cyber War." It's available on CSIS's website, but here are five key points and recommendations.

No. 1, cyber attacks are attacks. If they imperil life, health, 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.

No. 2, we need to adjust our risk tolerance. Ten years ago, it made sense to require high-level approval for offensive cyber action. The tool was new, we didn't really understand it. But now we have talented, brilliant cyber operators and we need to let them have their heads. It's really important to flip the risk calculus. The default answer to a proposed operation should be yes, and a naysayer should have to prove it is too risky instead of asking the operators to prove the operation is safe.

No. 3, we need to collaborate early. Cyber tools can be very effective in disrupting an adversary. We saw some of this in Venezuela just recently. But operators need time to plan. This is not a tool that just sits on the shelf and you reach out and grab it when you need it. They need to be incorporated from the very early stages of planning.

No. 4, run the playbook. The report lays out these steps in detail, but here's the key point: be bold. We can retaliate cyber for cyber, but we don't need to stop there. We need to match creative policy responses to the pain points of the particular attacker.

Then, No. 5, Congress should create and fully fund a cyber force. I know my colleagues are going to have other things to say about that, but this is something that I believe will actually close the gap faster than pretty much anything.

In conclusion, a dramatic change is needed in the cyber domain. The Trump administration's recently-released National Security Strategy did mention offensive cyber operations. I think that's a positive development. I would suggest a new policy, cyber first, cyber optional. We are redefining proportionality in the cyber domain.

Thank you.

[The prepared statement of Ms. Harding follows:]

PREPARED STATEMENT OF EMILY HARDING

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 cyber attacks have been muted, and escalation dominance does not exist.

The United States' 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 on-going, 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 cyber attacks, 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. policy makers 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 cyber warfare, one for which U.S. systems and policy are ill-prepared. To test how policy makers might respond in a massive cyber attack on U.S. territory, CSIS ran a series of war games. The results revealed the likely disastrous confusion that would occur in a cyber-first conflict, as policy makers 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:

- *Cyber attacks 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 United States prides itself on protecting innocent civilians, not targeting them, so it refuses to target civilian critical infrastructure. Therefore, a proportional response to a cyber attack on our critical infrastructure would be severe and likely include economic or military measures.
- *The United States will assume any cyber attack on critical infrastructure has a destructive intent and respond accordingly.*

Internalize the Shift for U.S. Decision Makers

Redefine proportionality and escalation to include the big picture. Policy makers' 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 cyber attack 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 time line, incorporating cyber tools in the early stage policy planning process. Then, policy makers 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 policy makers 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 cyber attack 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 tool kit 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 cyber attacks. For more, see CSIS's A Playbook for Winning the Cyber War.

Mr. OGLES. Thank you, Ms. Harding.

I now recognize Mr. Cilluffo.

Mr. CILLUFFO. It's a mouthful.

Mr. OGLES. Cilluffo, my apologies, for 5 minutes.

STATEMENT OF FRANK CILLUFFO, DIRECTOR, MCCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY, AUBURN UNIVERSITY

Mr. CILLUFFO. I am in violent agreement with my fellow panelists here and really happy to see that you are proposing such an important topic and one that I think is going to generate a lot more attention in the days ahead.

In addition to this question, the fundamental one, we really do have to start answering what that requires of our authorities, institutions, capabilities, and partnerships. Just last month, my institute released a significant report on many of these topics on offense, deterrence, and strategic competition. I co-chaired that, had the privilege of co-chairing that alongside Chris Inglis and General Frank McKenzie as well as at Tom Bossert. I suggest everyone take a look at that when you get a chance.

The summary, the conclusion was pretty straightforward. The status quo ain't cutting it and our adversaries are not operating episodically. They are operating persistently. Cyber space is an always on, always contested domain. China in particular, as my panelists have mentioned and you, Mr. Chairman, teed up in the very beginning, demonstrated this long-term strategic intent. Campaigns such as Flax, Volt, and Salt Typhoon are all really serious on their own. Taken together, however, they form a perfect storm. It's the pre-positioning at a time of their choosing that I think in U.S. critical infrastructure that is a line that has been crossed. Russia's experience in Ukraine reinforces the point, underscoring a hard truth. Our adversaries already view cyber space as a domain of continuous engagement.

Some of our approaches to tackle this, I'm a big proponent of National Security Presidential Memorandum 13, NSPM 13, and the adoption of the defend forward approach was an important shift, enabling greater agility and allowing U.S. Cyber Command to dis-

rupt adversary campaigns before they reach our shores. It's generated some genuine real operational benefits, but in itself it's not enough.

We've also seen more recently how cyber capabilities can be integrated with other instruments of national power for strategic effect and signaling. The Chairman of the Joint Chiefs, publicly discussing the role cyber played in Absolute Resolve, by all accounts an exquisite operation targeting the Maduro regime in Venezuela, makes this clear.

While public acknowledgment is relatively new, it is consequential. It underscores that cyber is no longer peripheral, but integrated, operational, and central to modern deterrence, and can shape the behavior not only of those targeted, but all those watching. At the same time, these advances surface unresolved questions about oversight, interagency coordination, escalation risk, and I'm very much with Dr. Lin is in terms of escalation, as well as the interaction between cyber operations abroad and defensive responsibilities at home. These are not academic debates. They go to the heart of democratic accountability and strategic stability.

One point bears emphasis. Offensive cyber operations alone are not sufficient to protect the homeland. When cyber action is taken abroad, it must be paired with strong domestic defense, led by DHS and CISA working with SLTT and private-sector partners to improve resilience across our critical infrastructure. But a purely defensive posture is equally insufficient, if not more so. Simply put, we cannot firewall our way out of this problem.

Deterrence in cyber depends on the interaction between offense, defense, resilience, and credibility over time, not reactive episodic responses built for a different era. In essence, we've let the adversaries define our strategy. We react and that becomes our strategy. That's unacceptable.

This brings me to the private sector. The vast majority, as we know, of critical infrastructure is owned and operated by the private sector. These entities are already on the front lines, yet are too often treated as passive victims rather than essential partners. Many of the most relevant capabilities from threat intelligence, rapid response, large-scale mitigation, reside in technology companies, cloud providers, and infrastructure owner-operators. In practice, the private sector already conducts elements of active defense. What remains unresolved is how far they should be permitted to go, under what legal authorities, and with what safeguards. Clarifying the legal and policy boundaries around lawful, proportionate, and well-governed active cyber defense would strengthen collective defense, raise adversary costs, and reduce ambiguity while preserving oversight and civil liberties.

There are a number of promising steps under way, from CISA's JCDC to NSA's CCC. But these efforts have to be reinforced by clear doctrine, modernized authorities, and governance structures. Net stakes are high as adversaries deepen their access into American networks. The United States must decide whether to remain constrained by outdated frameworks or adapt the realities of 21st Century conflict. Congress has a critical role to play in that recalibration by modernizing authorities, strengthening oversight,

and ensuring our institutions can operate with both agility and accountability.

Mr. Chairman, thank you for the opportunity to join you today.
[The prepared statement of Mr. Cilluffo follows:]

PREPARED STATEMENT OF FRANK CILLUFFO

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 United States more credibly deter adversaries in cyber space 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 2000's 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—prepositioning 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 cyber space 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 cyber space 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 cyber space. 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 cyber space 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

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-

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>).

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 toward 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. Last, 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 cyber space.

Mr. OGLES. Thank you, Mr. Cilluffo.

I recognize Mr. Bagley to summarize his opening statement, 5 minutes.

STATEMENT OF DREW BAGLEY, CHIEF PRIVACY OFFICER, CROWDSTRIKE

Mr. BAGLEY. Chairman Ogles, Ranking Member Thompson, Members of the subcommittee, thank you for the opportunity to testify before you once again.

Throughout my career, I’ve seen first-hand 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, I’ve had a front row seat to our defense of critical entities. This includes many components of the U.S. Federal Government, major technology companies, financial services firms, 43 of 50 U.S. States, critical infrastructure, and thousands of small- and medium-sized businesses. We defend America.

Today, unfortunately, many organizations remain undefended, vulnerable to cyber attacks, the scope and severity of which continues to increase. Simply put, threat actors are still operating at scale, still operating with limited consequences, and still all too often achieving their objectives. They are seeing a clear return on investment. Their risk calculus still shows favorable outcomes. To make durable progress, we must work in a concerted fashion to change each of these conditions.

The role for offense in confronting cyber threats is textured. I’ve outlined several elements in my written testimony, including the Enterprise Defender’s threat hunt across their own systems, resources, and data. This is a proactive approach, sometimes called

active defense, rather than offense per se, but it's one of the most effective techniques to confront targeted attacks.

Some suggest victims or their representatives should hack back. I've shared the history of this debate in my written testimony. But in short, hack-back operations risk revictimization and collateral damage. On-going investigations could be disrupted and retaliation could lead to waves of geopolitical escalation. For these reasons, offense is best left to professionals with relevant authorities, deconfliction processes, and clear oversight. A federated regime for hacking back that lacks these attributes probably creates more problems than it solves.

Let me state plainly that defense remains foundational. Even those who wish to increase offense must recognize the value of robust defenses. 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 and effective.

A core prescription for better confronting cyber threats is more focused, more persistent, and more tightly orchestrated campaigns disrupting threat actors and those who support them. JCDC, in concert with industry, should establish a most wanted style list. As a community, we should work our way down that list rapidly, performing disruptions and takedowns to frustrate adversaries' objectives and prevent them from reaching scale.

For criminal activities, we should apply laser focus on preventing monetization. Terrific work is done today, just not at a high enough tempo. Still, there remains a role for deterrence. Cyber attacks are caused by adversaries. Threats themselves are not deterrable. The people, institutions, and nations behind them often are. Given that their motivations vary so widely. There is no singular approach to deterrence that could succeed, but we should still use all available tools, including noncyber tools.

Policy makers face challenges in considering how to resource defense versus offense. Ultimately, it's probably reasonable to conceive of security investments as a portion of overall IT spending and reasonable to align offensive investments as a portion of overall military spending. AI impacts these considerations. AI provides threat actors with a new class of systems to target and acts as an accelerant to automate their TTPs.

AI itself is under threat from adversaries, meaningfully increasing the attack surface when left unprotected. Fortunately, AI detection and response solutions can prevent prompt injection, jailbreaks and model manipulation attempts. Agentic AI is already revolutionizing security operations to assist defenders.

To confront these challenges, I recommend the following. First, public and private organizations must take reasonable actions to defend themselves, with a focus on threat hunting and identity security.

Second, the cybersecurity community should radically increase the operational tempo of malicious infrastructure disruptions and takedowns. Given its stakeholder engagement functions, CISA should be central to coordinating public and private actors to this end.

Third, Federal law enforcement, along with Title 10 and Title 50 entities, should work to increase deterrence.

Finally, we must defend AI systems and leverage AI to defend enterprises.

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

[The prepared statement of Mr. Bagley follows:]

PREPARED STATEMENT OF DREW BAGLEY

JANUARY 13, 2026

Chairman Ogles, Ranking Member Swalwell, Members of the subcommittee, thank you for the opportunity to testify today. Throughout my career, I have seen first-hand 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 United States 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 cyber space. 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 on-line 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 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 CYBER THREATS?

America remains vulnerable to cyber attacks, 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.

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

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.

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 off-lining 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 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 CYBER-ATTACK 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. On-going 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.

³As 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.

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.

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 intra-domain (i.e., also a cyber attack) or cross-domain (e.g., leveraging a law enforcement or conventional military capability).⁴

Cyber attacks 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 cyber defense.

HOW SHOULD POLICY MAKERS 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).

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., cross-domain responses) to pressure adversaries, dampen their success, and prevent them from operating at scale.

⁴For 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.

⁵Whether other means to attain intelligence or other means to achieve effects.

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,⁷ there might be less focus on disrupting monetization and law enforcement actions, 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.

Everything I’ve described here does take place—just not nearly enough. It’s really a matter of will for decision makers 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 de-

⁶Our 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).

⁷Although not in the case of national state actors engaged in cyber crime 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.

⁸In 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.

⁹Such agents are central to a profound change that’s under way 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.

tection and response (EDR), threat hunting, identity threat detection and response, SaaS security, and cloud security as high-leverage areas of investment to this end.

- 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 CISA¹⁰ 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.

Mr. OGLES. Thank you, Mr. Bagley.

Members will be recognized by order of seniority for their 5 minutes of questioning. I now recognize myself for 5 minutes.

Again, I want to thank the panelists for being here. This is an important topic for us to be really bringing to the forefront of kind-of today's conversations and, quite frankly, the onslaught of media that we see every single day. When you look at the Monroe Doctrine, you know, our dominance in the Western Hemisphere, that is seen in the context of borders and boundaries. But now with the cyber and the AI landscapes, that would also include those boundaries and those borders.

So as we look to our capabilities, clearly Mr. Bagley, we need a great defense, threat hunting, and all the such. But when you look at the Typhoon clusters, we now are going to have to go on offense. We have to make the pain points significant for our adversaries to understand that if you breach the Monroe Doctrine, that if you break our hemisphere, our borders, our boundaries, there will be a price.

Mr. LIN, I want to start with the current state of play today. Offensive cyber capabilities exist across multiple parts of the U.S. Government under different authorities like Title 10 and 50 with varying degrees of integration with the private sector. As we look ahead, as the U.S. Government considers a more forward-leaning posture in cyber space, what actually exists today in terms of offensive cyber capability, who currently has the authority to employ it, and what are the most important questions Congress should be proud of prioritizing right now if we are to consider whether and how the private sector could be empowered to play a more direct role in offensive or cost-imposing cyber operations?

Mr. LIN. Thank you, Chairman. You know, I'll answer your question in two ways. No. 1 is around authorities. I think it's important and critical that, (A), as my, some of my co-panelists have said that we are cooperating hand-in-hand with the authority holders of Title 10 and Title 50. But it's important to remember that DHS, CISA have authorities of their own that ought to be used as well and

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

used aggressively here. We're talking about Title 18, we're talking about Title 14. Right? So the ability to use law enforcement authorities in combination in concert with Title 18—Title 10 and Title 50 is absolutely critical.

But No. 2, I think what needs to shift here is a mindset not just around doing episodic one-off operations of disruption, which are important and critical and can be successful, have been proven to be successful, much like the KB botnet takedown that the FBI led recently. But what does it take to match the speed and scale of our adversaries? To match the scope of what it is that they are conducting against us? One-off episodic operations, while important for deterrence, will never be enough to change the cost calculus of our adversaries.

Mr. OGLES. Exactly. Well said.

Ms. Harding, recent reporting indicates that a PRC-linked cyber actor, commonly referred to as Salt Typhoon, targeted systems supporting Congressional committees. This was not a private company or an Executive agency. It was the Legislative branch of the U.S. Government. From a strategic standpoint, what message does it send when a nation-state is willing to target Congress directly? Should this committee view that as a clear evidence that current approach to deterrence in cyber space is insufficient?

Ms. HARDING. In a word, yes. I would want to draw a distinction, however, between an intelligence operation and a disruptive operation. As a former intelligence officer myself, I have to sort-of tip my hat to Salt Typhoon. They have been very clever, very talented. They have proven just how good China is at its current cyber activities. Going after Congressional staff from an intelligence perspective is a logical target. In my last role on the Senate Intelligence Committee, we frequently gave defensive briefings to our fellow staff and to Members of Congress to explain just how much they would be targeted and how sophisticated the adversaries were who were coming after them.

Ideally, yes, you'd be able to establish deterrence in an intelligent sense and you'd be able to say, OK, if you penetrate our networks, then you will feel consequences for that. It also is sort-of a normal spy versus spy, tit for tat.

A very clear distinction, however, is between the Salt Typhoon kind of activity and the Volt Typhoon kind of activity. There is zero intelligence value in penetrating water networks, power networks, especially around military bases. That is there for one reason and one reason only: to disrupt the United States military in the case that we had to deploy suddenly. If there were to be a Pacific contingency, a 6-hour delay, an 8-hour delay, a 12-hour delay could be definitive. If sailors can't get to their ships, if you can't load the ships full of equipment, then that is a 6-hour delay, an 8-hour delay, a 12-hour delay. It's a smart act for, I think, a potential adversary to take, but it is one we may not allow. We have to be able to deter that kind of activity and strike back.

Mr. OGLES. Thank you.

I now recognize the Ranking Member, the gentleman from Mississippi, for 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Chairman. Very rarely do I find witnesses with very little difference in testimony, so I compliment you on that.

But if our national cybersecurity strategy is going to shift toward a more aggressive offensive cyber strategy, we will need to ensure that the agencies responsible for such efforts, such as U.S. Cyber Command and the National Security Agency, have the staffing and resources necessary to carry out offensive cyber operations. Yet both Cyber Command and NSA have had personnel reductions over the last year.

All of you have talked about capabilities. I mean, if you are going to fight an enemy, you need the ability to do that. So in your analysis, are we in a position, given the current staffing, to say that we are at a point where we are good or the cuts have vulnerabilities that we should address at this point?

I will start with you, Mr. Lin, and we will go down the line.

Mr. LIN. Thank you, sir. I can't comment on the specific force structure or even the numbers that we necessarily need in each of these organizations, but what I can say is this: we will never have enough people if we're simply trying to throw more people at the problem against our adversaries. Our adversaries outnumber us 50 to 1 or, in some cases, 100 to 1. So when we think about what is the future of staffing structures, force structures, whether we're talking about for Cyber Command, for NSA, for DHS, we have to approach this problem from the perspective, of course, of thinking about what's the level of human expertise and oversight and control that's needed, but also what are the technologies that are needed that enable our people, our war fighters, our officers, to operate at scale against an adversary that has a quantitative advantage against this, and that exceeds orders of magnitude.

Mr. THOMPSON. Ms. Harding.

Ms. HARDING. Thank you, sir. You're absolutely right that a lot of very talented people have left the Government, and there is concern there. I think the question is right-sizing and having the right talent in place to be able to fight back against these particularly talented and committed adversaries.

Cyber force, so I think at least three of us up here are in favor of the creation of a cyber force. That is because we need to think about this talent differently. We need to think about this force structure differently. This is not necessarily, you know, picking up a heavy rucksack and a hundred pounds of batteries and running through a field. Instead, this is a very specific set of skills, and we do want to lean heavily into a reserve cadre for cyber force. We have lots of talented people in the private sector, two of whom are sitting right here at the table with me, who can contribute both to the U.S. Government in a military sense and also in their private day jobs. Israel is perhaps an example to look at for this. They do this exceptionally well, where they blend together their private sector and their military activity so that both benefit, frankly.

I would also encourage, especially given this committee's jurisdiction, to take a hard look at the Coast Guard. They have a spectacular set of authorities and a really interesting cadre of cyber operators that can do all kinds of things that you wouldn't necessarily expect. That's kind-of a latent cyber power that I don't think we

give enough credit to right now. Also, the National Guard. There are quite a few National Guard units, especially in places that are obvious, like Maryland, that have real talent in this space. They have clearances, they have capabilities, and they could play a much bigger role, especially in homeland defense, than we're currently allowing them.

Mr. CILLUFFO. Mr. Thompson, just very briefly, I would support Emily's comments there. Yes, we've lost some people. We're never going to have enough people. But I think there's some issues we need to get our arms around quickly. Some of them may not be sexy, but they're actually important.

Cyber is not—it is its own domain, but it transcends all other domains: air, land, sea, space. Until we integrate computer network attack and cyber into our war-fighting strategy and doctrine, we're going to be hamstrung. So part of that is making sure we have the structural capabilities, that we have the women and men that can help make that happen. Part of that is ensuring we have the political will, because deterrence only works if it's consistent and if it's credible.

Here's the truth. If you look at how we've responded thus far, we've, in essence, been blaming the victim. An incident occurs, who do you blame? You blame the company, you blame the critical infrastructure, owner, operator? Yes, they need to do more. But how many of these companies went into business thinking they had to defend themselves against foreign militaries and foreign intelligence services? It's an unlevel playing field. So I think consistency, credibility, and signaling that there will be consequences for bad behavior is essential.

Mr. THOMPSON. Thank you. I appreciate the Chair allowing Mr. Bagley to answer the question.

Mr. BAGLEY. Thank you, Mr. Chair. Thank you, Ranking Member Thompson. I think fundamentally we should think about what we all discussed today as being a call for cross-domain responses at times. Sometimes we'll confront cyber with cyber, sometimes there'll be cross-domain responses.

So in terms of resourcing, I can't speak to the appropriate number of personnel. I think those in charge of agencies are best able to speak to that. But I can say we should want CISA to succeed, for example, and to have the processes and the technology they need. Then to make sure this subcommittee, through its oversight powers, is ensuring they have the personnel they need to succeed in that mission. But we should also be thinking expansively, as my colleagues have suggested, about other capabilities and other agencies throughout the Government. Because when we are trying to change adversary behavior, sometimes it's going to take authorities that are outside of the realm of what we think about with CISA or DHS in general, and instead we're going to be thinking about diplomatic tools, economic tools, law enforcement tools, or even military tools. So I think we should think expansively about that and work backward from that problem set.

Mr. THOMPSON. Thank you. I yield back, Mr. Chair.

Mr. OGLES. Thank you, Ranking Member.

I now recognize Mr. Fong for his 5 minutes of questioning.

Mr. FONG. Thank you, Mr. Chairman. I want to thank the panelists. This certainly builds upon the previous committee hearing that we had, when we talk about how we are seeing our foreign adversaries weaponizing AI and quantum tools to automate cyber espionage campaigns against the United States and soft targets, as mentioned before.

I do want to delve into this cyber force, cyber talent conversation. You know, certainly we are seeing universities and we are seeing community colleges try to develop a pipeline when it comes to teaching students cybersecurity tools and the technology.

I kind-of want to get your thought, Ms. Harding, in terms of, you know, as Mr. Lin had talked about, we don't have enough people compared to our adversaries. But how do you—what is your perspective on how we need to invest in our universities and community colleges in terms of developing that cyber talent?

Ms. HARDING. So universities and community colleges are very important. I think we have focused a lot on certifications for cybersecurity, and that's important. But what we really want to push forward in the future is capabilities in AI, understanding how that's going to really change the landscape, and then also just sort-of a creative thinking. Some of the best cyber operators are not the ones who are the best coders. They're the ones who have the best ideas and the guys who think like the adversary, the guys who can come up with creative ways to get around obstacles, if they find them. These are the people who do the biggest, baddest cyber operations, and it is a thing of beauty to watch.

I think that, you know, we can think about the talent pipeline in the kids who are coming up now. We also really need to think hard, especially in this moment where we do have this meeting of the minds between Silicon Valley and Austin, Texas, and Washington, DC, where this is an important skill set to welcome people into the Government in a part-time capacity. You were a Navy Reservist. This is a great model. If you have people who can serve in the military reserves, serve in a cyber capacity, take the skills they've learned in their private-sector positions, and then pull them into the Government, like that is ideal.

Mr. FONG. I think that is an important point, which is if we need to be training and teaching students differently in terms of not just on just a cybersecurity defensive posture, but to look at how do we make our technologies more robust, this is something that as universities and community colleges start developing their curriculum, we might need to have a conversation about how we get—if universities and community colleges are going to develop these programs, actually have them train students to actually meet the demand and the needs that our country needs. So I would love to continue that conversation.

I would like to ask Mr. Lin, when it comes to information sharing, certainly with your expertise, private-sector cybersecurity firms often possess earlier and deeper visibility into our adversaries' infrastructure, attack paths, operational patterns than the Government systems alone. Based on your experience, how is information sharing now and what barriers exist currently that we need to address to ensure that we have more robust coordination?

Mr. LIN. Thank you, sir. Let me answer your last question first, which is how is it now? It's certainly improved considerably from 10 years ago or even 15 years ago. What you alluded to is spot-on, which is that these days private-sector companies, especially those in the cybersecurity domain, have extraordinary global sensor networks that rival those of even other intelligence—signals intelligence agencies. So it makes enormous sense for there to be very robust information-sharing bidirectionally and it has to be bidirectionally. We have to have—we have to make it possible, easy, and we have to encourage private-sector companies to share what their sensors are seeing as holistically as possible with our intelligence agencies, and it has to go—and vice versa. When we are able to downgrade intelligence that we're seeing through our robust signals intelligence apparatus, we have to be willing to share that with our private-sector companies as well. Go ahead.

Mr. FONG. Yes.

Mr. CILLUFFO. Mr. Fong, just because I think the committee itself should be applauded for the PILLAR Act pivot, I mean, these are essential to be able to move forward. But I think to your point earlier, it's not just the traditional rote learning in a classroom. You need to give students opportunities to be in applied environments where they're actually engaged. Because I'm telling you, most of the best in the cyber community are not learning it in the classroom, they're learning it in the real world. I think looking to ways where we can build co-ops, we can build new opportunities with both industry and Government will be absolutely essential for success.

I would just add on the information-sharing question, we've been around this issue for 25 years. Here's the truth. We've got to move beyond information sharing to operational collaboration. Until we get to that stage, we're always going to be marching into the future backward. That is always by definition reactive. We need to get to the point where it's combined. You're in the same foxhole and you're fighting the same fight and you build the trust, which is everything. It takes years to build, nanoseconds to lose.

So I just needed to jump on that. I'm sorry for jumping in here.

Mr. FONG. Oh, I appreciate that. This is a very—

Mr. CILLUFFO. Random unspoken thought, sorry.

Mr. FONG. This is a very important topic and we need to continue the conversation.

Thank you, Mr. Chairman, for your leadership in putting this panel together. Thank you. I yield back.

Mr. OGLES. The gentleman yields back.

I now recognize the Member from New Jersey, Mrs. McIver.

Mrs. McIVER. Thank you, Mr. Chair and Ranking Member, and thank you to our witnesses for being here today.

I just want to quickly express my condolences to the family of Renee Good as well. What happened in Minneapolis, where she was fatally shot by an ICE agent, is horrific and deeply troubling. My thoughts are with her loved ones, especially her children, and with those affected by this tragedy as many in this country continue to mourn and seek answers.

As we discuss Trump's reliance on offensive cybersecurity tools, we must ask whether we are prepared to use these tools respon-

sibly. Cyber offense depends on a strong, well-trained work force, not only to conduct operations, but to manage consequences and defend against a counter attack. Today we face a serious cybersecurity work force gap, which has been discussed in depth by many of our witnesses. We lack enough individuals to protect our infrastructure, economy, and national security. Expanding offensive tools without the people to sustain and defend ourselves is not deterrence, it is a risk. We must ensure that our home is secure. We must have the personnel and resources to fight any cyber threat before we dedicate time and resources to provoking malicious actors and cyber offense.

With that, many of our witnesses, especially Ms. Harding and Mr. Bagley, talked a lot about what we need to do in order to increase work force. Would love to give you guys a few moments just to talk about some of the barriers. How do we remove some of the barriers that we see right now with folks trying to join the cybersecurity work force?

I can start with Ms. Harding. Ladies first.

Ms. HARDING. Why, thank you, ma'am.

So some of the barriers that we see, No. 1, is a barrier of imagination. I think there are people who think, you know, oh, that's going to be technical, that's going to be hard. I can't do it. There are some great programs to reach out to communities that maybe don't see themselves in this world, and those should definitely continue. There's some women in STEM programs, for example, that are really tremendous.

I think also, you know, when people think about the intelligence community, they think about that as a certain type of person that you've got to be really straightlaced. You've got to be, you know, the kind of person that has a buzz cut as opposed to the kind of person who has purple hair. It's just not true. I think welcoming a wide variety of talent into the Government is really important. You know, I say to people all the time, are you interested in doing really, really sneaky and sometimes illegal things in the cyber world? Join NSA. This is what they do and they do it very well. I think there's some real opportunity out there that maybe it just doesn't occur to people.

Another one of the barriers that we should really think through, I think, is going to be this coders to the AI space. So it's going to be a sea change. I know that you'll have more to say about this, but, you know, we've trained people to do really excellent jobs coding. In this strange new world we're going to have AI doing a lot of this work for us, and we're going to have a dearth of talent that really understands the way that AI works both for offense and defense.

One of the things that I would really love to see the Government put in place as well on the defensive front that you were talking about, that we really need to secure and be more resilient at home, is to create kind-of a Teach for America, but in the cyber realm. So the Government perhaps funds some training for people and in return you give 2 years back where you work in a school system, you work in a rural area, you're responsible for cybersecurity in a whole raft of rural water treatment facilities. You then repay what—the loan you got basically to go to school and you give to

communities that are desperately in need of strong cyber talent to build a better defense.

Mrs. MCIVER. Yes, thank you for mentioning that. I am a big supporter of Teach for America coming from a school district and working. It is a great program and offers great incentives that brings many talents from across the world to work in these school districts. So thank you for that.

Mr. Bagley.

Mr. BAGLEY. Thank you. I think with my limited time, two primary ways we should think about this are, No. 1, with pathways, but we shouldn't think about pathways only being at the beginning of the career cycle. Instead, there should be more return to work programs where those who have taken time out of the work force, such as to be a caretaker or those who have taken a different career path, still have a path back into cybersecurity.

The second, and I think that enables the first, is really this upskilling we're seeing with AI. Now that we have this notion where a lot of automation can occur and we're really relying upon talent to have wisdom and do good decision making, we're no longer relying upon the same set of skills that would have taken years and years to learn when we were talking about coding from scratch. So I think that's something we should really leverage as an opportunity to bring more into the work work force.

Mrs. MCIVER. Thank you so much.

With that, Mr. Chairman, with that, I yield back.

Mr. OGLES. The gentlewoman yields back.

I now recognize the gentleman from Florida, Mr. Gimenez, for his 5 minutes.

Mr. GIMENEZ. Thank you very much, Mr. Chairman. I am sorry I wasn't here for the testimony, so maybe some of these things have been answered.

You know, if I were a CEO of a large corporation constantly being attacked and constantly being attacked, you know, from what I am reading is I have limited capability of hitting back, correct? Yes. That would be an itch that I really want to scratch. OK. So has there been any thought of creating—I mean, some of our corporations have billions and billions of dollars, you know, probably way more capable than we are, OK, in terms of resources, of creating some kind of a private-government, you know, offensive team that would allow me to satisfy my itch, OK, and hit back at some of these people that are hitting me all the time? Has there been a thought to do that? Do we have something like that? Anybody can answer.

Mr. BAGLEY. Sure. Thank you for the question, Congressman, and good to see you again. I think, importantly, JCDC does possess the ability to nominate campaigns and to nominate campaigns to those with Title 10 and Title 50 capabilities to be able to engage in appropriate activities such as taking down adversary infrastructure, such as doing some sort of activity that would, hopefully, deter and change that behavior. So I think that's the appropriate mechanism.

So I think, if anything, this is something where there should be, as I noted in my written testimony, there should be something akin to a top 10, a most wanted list, perhaps it's more than 10, but a

most wanted list. That's the mechanism by which companies, organizations, nonprofits, academia, those affected, those impacted, can work through JCDC, get those that have a high impact nominated, and then using existing capabilities can, at a high tempo, go after these sorts of adversaries.

Mr. GIMENEZ. So that we can kind-of control who it is that we are going after, the Government controls who control who we are going after. It is like a bounty. You are a bounty hunter.

Mr. BAGLEY. It's a public-private collaboration.

Mr. GIMENEZ. OK. All right.

Mr. CILLUFFO. Mr. Gimenez, if I could just expand on that. I think this is a significant issue and an important issue and I think time to really address this particular matter. In addition to JCDC, the National Security Agency has its Cybersecurity Collaboration Center, which coordinates with the defense industrial base. I think there is an opportunity to get to genuine operational collaboration. I don't want Yosemite Sam shooting all over the place. But at the end of the day, think about it as suppressive fire. Think about it in a football context. You have offense, you have defense, you have linebackers who blitz the adversary, the other team's quarterback.

So all things said and done, I think we need to get to that point and I think there are some authorities questions that need to be answered. But your itch is my itch and it's been there for a long time.

Mr. GIMENEZ. I like your football analogy since I am a big Kane fan. OK? We're in the National.

Mr. CILLUFFO. I have two daughters who went to Miami, so I know they've got their NIL money.

Mr. GIMENEZ. The question that I have is that, you know, we have the criminal element, that a lot of it is based overseas, a lot of it based in some adversarial countries. Do we have evidence that those adversarial countries are actually working with those criminal elements inside to hit us? Do we have any evidence that they actually get a cut of whatever it is that those criminal elements do get? Open-ended question to anybody wish to answer.

Ms. HARDING. I'll start on that one briefly. It's a complicated answer to what seems like a very straightforward question.

In the sense of China, we are seeing more sort-of popping up of criminal networks that seem to be government people who are moonlighting on the side at night doing criminal activity. But China's pretty locked down. They like to control their people and what they're doing, so it's sort-of a tight ship that they run.

Russia, on the other hand, is a very different story. We see more of an atmosphere where there's a commander's intent. You know, Putin wants this particular adversary to have problems, go forth and make it happen. There's kind-of a deal that happens between a lot of Russian criminal networks and the Russian state, where the Russian state says, you're going to operate outside of Russia, you're going to make life hard for our adversaries. We're going to ignore the criminal activity that you're doing and allow you to operate. But if you get cross with us, then we will come after you and arrest you on a moment's notice.

Mr. GIMENEZ. Do they get a cut?

Ms. HARDING. I'm sorry?

Mr. GIMENEZ. Does the Government get a cut of the profit of the criminal activity?

Ms. HARDING. There's probably some interesting work to be done following the money there. I mean, in Russia in particular, there's a lot of corruption. Right? So, yes, you know, do you get a kickback for allowing criminal activity to go on? I would assume so. But you'd want somebody to really get in deep and follow the money there.

Mr. GIMENEZ. My final comment is going to be if we continue just to play defense and play defense and play defense, we are just inviting attacks. So we need to go on the offensive and really whack them. As hard as they whack us, we need to whack them twice as hard so that this stuff stops.

With that, my time is up and I yield back. Thank you.

Mr. OGLES. The gentleman yields back.

I now recognize the gentleman from Virginia, Mr. Walkinshaw, for his 5 minutes.

Mr. WALKINSHAW. Thank you, Mr. Chairman. I want to add to the condolences for the family and loved ones of Renee Good. She had 3 children, including a 6-year-old, who are all without their mother today.

Mr. Chairman, thank you for convening today's hearing. You beat me to the punch on the sports analogies. You are right that the best defense is a strong offense. I think it is still the case, however, maybe arguable, that defense wins championships. The Commanders have no offense and no defense, but I think both are still important. Yes.

A talented work force combined with a Federal IT infrastructure that embraces cutting-edge technologies, I think, should be the foundation of our efforts to counter cyber threats and to maintain an offensive cyber posture or grow our offensive cyber posture. It does trouble me that last year a third of the work force, and this has been noted by others already at CISA, which is our leading agency to deter threats to both our cyber and physical infrastructure, was wiped out by DOGE. In the recent shutdown, staff at CISA received RIF notices. Turned out those notices were illegal, according to courts, and a lot of them were moved to ICE and CBP to engage in immigration enforcement efforts. So these staffing cuts have left a big hole in our cyber defenses, our ability to combat attacks from Iran, Russia, the PRC, has been noted.

Mr. Bagley, in your written testimony, you analogized cybersecurity to physical security and you made the point that in a city, even with a very successful crackdown on crime, where law enforcement is going out and arresting the bad guys, still prudent to lock your door at night. Unfortunately, in my view, the firing of many of our cyber experts unlocks and opens some of our doors. So I am hopeful that will be reversed.

One of my concerns is the administration's elimination of the Multi-State Information Sharing and Analysis Center. It was a critical tool for decades for State and local governments, especially small, rural local governments, who maybe didn't have their own resources, our capacity to have visibility into the cyber threats that they face. I think it is the case that even if we want to be more aggressive in terms of our offensive cyber posture, we have to start

from a place of visibility into the threats and cyber attacks that we are facing, especially State and local governments, which, as a former local government official knows, a lot of the personally identifiable information of every single American is held by State and local government. So the loss of that capacity concerns me.

I want to just dig in a little bit, and there has been a lot of agreement, but, Mr. Lin, you said in your testimony our offensive cyber utilizes bespoke teams, not at an industrial level, kind-of limited in your view. Ms. Harding, you said the U.S. offensive cyber capabilities are strong, perhaps unmatched in the world. A little bit different analysis there. I only have 1 minute, so maybe I will give you each 30 seconds to let me know whether you all disagree or agree.

Mr. LIN. Yes, sir. Not contradictory.

Mr. WALKINSHAW. OK.

Mr. LIN. What I would say is this, which is, yes, we have some of the most talented cyber operators in the world, highly committed to the mission, very, very creative in terms of what they're able to pull off. I think we've seen perhaps a little bit of evidence of that in the last couple months. However, to what extent can they actually conduct those types of operations at scale? That is fundamentally what we're talking about here. Can they conduct those operations at speed and scale versus episodically? In cases where—in those cases does it take months or perhaps even years of planning to be able to pull off what they did?

Mr. WALKINSHAW. OK. Ms. Harding.

Ms. HARDING. Again, not contradictory, right. I think one interesting case study was the SYMPHONY exercise that we did a few years ago against ISIS in Syria. You can read through that and see just how many layers of approvals had to take place in order for that operation to come off. Now, things have changed since then, but it's really important to note that it's not necessarily—I mean, you could have 100 people or you could have 10 people running an operation. If it takes them 4 months to get the approvals they need to actually execute on the operation, then the opportunity is going to go. They're going to miss it. So it's—we are the most talented. We, also, I think need a more robust capability.

Mr. WALKINSHAW. Thank you. Thank you, Mr. Chairman.

Mr. OGLES. The gentleman yields back.

You know, to continue the sports analogy now, I think we are, when you look at cyber capabilities in this rebuilding phase where we need that better collaboration, we need quality versus quantity, we need those force multipliers, which includes the private sector, that is the way forward.

With that, I recognize the gentleman from New York, the Chairman of the full committee, to use as much time as he needs.

Mr. GARBARINO. I wish that was the case. Thank you very much, Chairman. Thank you very much for all witnesses for being here. To admit you are a Jets fan is very—I mean, it is a difficult thing to do every year and watch them every year. It is very difficult. But, yes.

Ms. Harding, I have a question with you. If the United States adopts a more forward-leaning cyber posture, including the use of private-sector capabilities, to disrupt or impose costs on foreign ad-

versaries, what should the operational role of DHS and CISA be when retaliatory cyber activities targets the homeland?

Ms. HARDING. Right. So what we've heard from the private sector, sort-of through the evolution of CISA and DHS, is that they see them as the good guys. When FBI shows up and asks a lot of questions, you know, they want to be helpful, but they're also there to look for criminal activity and to prosecute the criminals. That's a very specific skill set. When they talk to CISA, when they talk to DHS, what they're really feeling like they're getting is more of a partner.

I think the, you know, the JCDC had its upsides and its downsides, but it was, in fact, doing a lot of good trust-building with the private sector and it was a place to collaborate. I think that trying to adapt that, to adjust that, to moderate it for the future is really important.

Then what we were talking about with the two-way information sharing is absolutely critical. I think that the—one of the criticisms that DHS frequently gets is that, you know, you, you have your one person who you get cleared at the secret level and they go in and they get a briefing and they're like, that's it, that's all you're giving me? I could have read that in the *New York Times*. So we need to be more aggressive in sharing some intelligence information that we have. That's hard for me to say as a former intelligence officer, but I do think it's important.

Mr. GARBARINO. No, absolutely. That is one of the—you know, I have been between Ranking Member and Chairman for the last 5 years on this committee. The one thing I have heard repeatedly from our partners, private sector and allies overseas, is we are very good at taking information. We are very not good—it is not a one-way street. We are not good at sharing information.

Ms. HARDING. Exactly.

Mr. GARBARINO. Just to follow up on that, does DHS and CISA currently have the authorities or network access or operational agility required to move in that direction if that is where we go?

Ms. HARDING. I'm sorry, you're asking if DHS has the capabilities to conduct offensive cyber activities?

Mr. GARBARINO. Well, I mean, does CISA have the authorities necessary to do it or do we have to give them more authorities? Do we have to give them more access to—is there action that we need to do so the private sector can work with these partners in CISA?

Ms. HARDING. Yes. I mean, I think that there's a sort-of patchwork of authorities out there that you can cobble together to do some pretty impressive things. But I think looking at it from a zero-based standpoint and saying what we want to achieve here is really tight collaboration between the Government and the private sector, and what we want to do is take the best athlete from each team to sort-of continue the analysis. What can we do to make that happen and to really let the private sector shine in the things that they're very good at? I expect my co-panelists might have some other thoughts about the specific authorities of DHS, though.

Mr. GARBARINO. Sure. Jump in if you want.

Mr. LIN. If I may, one of the other things that I would add, right, is that we have to start thinking about cyber as a core element of multi-domain operations. So when HSI is conducting investiga-

tions, they should have the ability, the authority, the resources needed to be able to leverage cyber capabilities as part of their work. When Coast Guard is conducting missions, given their unique authorities, as my panelists have said, they should be able to leverage, they should have the capabilities and the tool sets needed to be able to leverage cyber, offensive cyber as part of their core responsibilities.

Mr. CILLUFFO. Just to build on that, Mr. Chairman, is—I mean, Emily brought up JCDC. I think JCDC, again, pros, cons, but in the event of a crisis, they're actually quite good. Bombs start dropping in Ukraine, they can get critical infrastructure owner-operators together, they can start sharing information. But it's episodic. It's only when there is a big event. What is that daily battle rhythm?

I mean, go with the sports analogies, which I started, sorry, but at the end of the day you got to put the reps in. You're not going to suddenly become a five-star recruit if you haven't been in the gym and on the field for years. So I think there needs to be something there that allows it to succeed not only in a bad day, but every day, so you're ready for that bad day.

I think, Mr. Gimenez, I am very much at the point where I think there are some authorities and some protections that are needed. First, WIMWIG, you got to get that over the goal line. That is essential. You can't trust the Government's going to lose all confidence of the private sector if we can't even get the basics. Imagine kicking us back a decade. That's what we're looking at here. That's unacceptable. So thank you for your leadership there. But I think just as importantly, you do need to also look to what that combined operation could look like from a collaboration standpoint, not industry on its own, in conjunction with government.

Mr. GARBARINO. Absolutely. I ran out of time. In fact, I would let you add on and I will yield back. But as for WIMWIG and PILLAR, those are two things that we are making a hard push. I believe the Minority is also making a hard push as well as the Senate Minority to get included in our final package next—instead of just a blank extender or a short-term extender, to get actually the bills done in next week's final package. But we will see.

With that, Chairman, I yield back.

Mr. OGLES. The Chairman yields back.

I now recognize the gentleman from Rhode Island, Mr. Magaziner, for his 5 minutes.

Mr. MAGAZINER. Thank you, Mr. Chairman. I also want to start by offering my condolences to the family of Renee Good, especially her children, who are going to have to live the rest of their lives without their mother. You know, we have a long history in this country of protest and civil disobedience. Those who engage in protest know that there can be consequences for doing so, but those consequences shouldn't be a death sentence.

I had an opportunity to attend an event over the weekend with all the police chiefs across Rhode Island, several of whom came up to me and said that the tactics that they are seeing increasingly being employed by Federal agents and immigration enforcement are tactics that police departments stopped using years ago. One of the things that I think we need to do as a committee is exercise

our oversight responsibilities to see what the leadership level at DHS is instructing its agents and officers in the field to do, because if they are not getting the proper training and guidance, not only does it do a disservice to the civilians who are being put at risk, but also to the officers and agents themselves.

Now, that being said, I am very glad that we are having a hearing today on this topic, and I thank you, Mr. Chairman, on the topic of how we deter and disrupt cyber attacks in the United States, because it has often occurred to me that these attacks are happening at increasing frequency and increasing brazenness. When I ask what the consequences are when foreign actors and other adversaries conduct these attacks, there don't seem to be any. We do need to have, I think, a serious retooling of the way that we think about this. If there are malign actors out there that continue to attack us in the cyber domain, we need to have the ability and the intent to disrupt their ability to continue to do so, period.

This is a little bit of a difficult conversation to have in an open setting. One of the things that I was going to suggest, Chairman, is perhaps we could continue this conversation in a Classified setting at some point so we can get into the weeds of what some of the different offensive deterrents could be in a way that we don't want to project publicly. But I just want to ask our panelists at a high level, when we think about what the parameters should be in terms of our offensive cyber actions to disrupt these threats, what are the sort of boundaries that we want to give not just to our cyber warriors, but that we want to project to the rest of the world? Keeping in mind that we are in an open setting here.

I notice, for example, Ms. Harding, you wrote in your testimony, "The U.S. prides itself on protecting innocent civilians, not targeting them. Therefore, a proportional response to a cyber attack on our critical infrastructure would be severe and likely include economic or military measures." So, like, I will start with you, and I will give the others a chance to weigh in, when you think about what the boundaries should be, what should be off-limits, what we want to project our boundaries as being, how do we think about that?

Ms. HARDING. So we have always prided ourselves in trying to protect civilian life. You know, if you're an innocent bystander, you shouldn't be wrapped into the political fighting that's going on and then the actual fighting that's going on. So I think that a clear bright line is civilian critical infrastructure. You know, if you are shutting off the lights in a city, hypothetically, for a military action, that's one thing, but the lights came back on. This is not, you know, dropping Kyiv into winter without any power and without any heat, that should be a very clear bright line.

I think that part of what we're all saying here is that we need to stop thinking about cyber as the thing that's over here in a silo. We need to think about it as fully integrated in the full range of policy measures, and we don't necessarily have to respond to an attack on critical infrastructure with an attack on critical infrastructure. We're the United States of America. We have other options.

Mr. MAGAZINER. Would anyone else like to weigh in on this question? Yes, Mr. Lin.

Mr. LIN. Thank you, sir. If I may, two thoughts.

No. 1, I would like for us to get to a place where we're not thinking about retaliation because we have done such a good job of being proactive in disrupting adversary operations well before they're able to conduct attacks against us. That's No. 1.

No. 2, what you are alluding to, sir, is the fact that there is this very perverse cost calculus for our adversaries. They have every incentive to go on the offense against us. There is no punishment. There is no cost. So the question that we should be asking, the objective is, how do we insert enough friction to drive up the cost, to change their cost calculus such that they're not thinking about offensive cyber operations as something that is easy to do, that they reap all the benefits from, and suffer no consequences for?

Mr. MAGAZINER. Yes, that makes sense. My time is running out, so I will just say this. I agree and I think this is an important conversation for us to be having. We also have to anticipate that our actions could provoke reactions and so we will need to harden our defensive cyber capabilities as well. That is why it is so important that we staff up and fund CISA and other agencies tasked with cyber defenses, not defund them, not shift resources away from them, as, unfortunately, I think has been happening over the last year. So, but directionally, I think everything that you all are saying makes a lot of sense.

With that, I yield back.

Mr. OGLES. The gentleman yields back. Mr. Magaziner, to your point, one of the things that I am working on is a roundtable approach where we can gather industry experts and then we would have that in the SCIF to allow for more both frank conversation, educational back and forth, because it is critical.

You know, as you see the kinetic action that took place with Maduro, I think we unveiled technologies that probably caught our adversaries off-guard, which means that the cyber attacks are going to escalate now. So there has to be that cost-benefit analysis of if you move ahead, what is the penalty for your country, for, you know, whatever group or organization that is attached to Russia or China?

But, you know, sticking with that, when you look at our current—you know, we have relied on attribution, sanctions, indictments, defensive improvements, which is critically important to respond to state-sponsored activity. You know, we see Chinese and Russian campaigns continue with increasing persistence and confidence. In your judgment, what actually changes adversarial behavior in the cyber space?

So let's go down the line. You know, Mr. Lin, we put you in charge of cyber force. Your job in charge is to protect the United States of America, to implement the Monroe Doctrine, to make it clear that the Western Hemisphere includes the cyber realm. What do you do next, sir? Ms. Harding is ready.

Mr. LIN. A couple things. Let me start by adding an additional observation, which is that what we're seeing from our adversaries is wholesale adoption of artificial intelligence for the purpose of offensive cyber. You can be—the hearing, sir, previously where that was soon after this was disclosed by Anthropic, where they discovered that state-directed PRC threat actors were abusing their models to be able to conduct operations against American targets, both

Government and commercial, there has to be wholesale adoption on our end. Smart, well-regulated, governed, thoughtful, but wholesale adoption of artificial intelligence capabilities merged in with modern software that we're using to, first, equip our soldiers, our warfighters, with the capabilities to be able to operate at the speed and skill that's needed in order to compete in this domain. If we're single-threading operations, we will be losing. That's No. 1.

No. 2, we have a lot of authorities in place. Again, I think some of my panelists have mentioned this before, which is there has to be a will, a political will, to employ these capabilities against our adversaries.

Mr. OGLES. Ms. Harding.

Ms. HARDING. So I love thinking like the adversary, and I like trying to figure out how we can hold to American values and morals, but still really mess with the other guys. Disruption, I think, is the No. 1 point. If you unleash our cyber operators, where the minute they see some adversary activity on a particular node, they can go after that node and shut it down. That's key.

A critical point in this is actually incorporating our allies. As you know, the internet is global. It's not just one point. Right? It actually touches on a lot of different things. You need to have a bunch of allies in place that can say, yes, I'm in favor of this. Let's go do it.

No. 2, we've gotten really good at very targeted activity. There's no real reason to go after an entire network if you know exactly where the bad guys are operating and you can mess with them specifically. I think more about that in closed session would be good.

Then finally, rapid response is really important. Right now our cyber operators are frequently asked to do things on a time scale that's just impossible because they haven't been given the time and the opportunity to actually build a tool kit. I think we do need more people and we also need more authorities to go and build those things ahead of time so that when something happens, there can be a very quick, punishing response to create that deterrence.

Basically, to sum it up, unleash the cyber operators. Let them play.

Mr. OGLES. We will pause there and we will come back to you, sir, in just a moment. But I would like to recognize the gentleman from Texas, Mr. Luttrell, for his 5 minutes.

Mr. LUTTRELL. Thank you, Mr. Chairman. Forgive my tardiness.

Good morning, everyone. I will throw this one probably Mr. Bagley, but Ms. Harding, you can jump in on it as well. I would like to talk on undersea cabling. Defensive, offensive posturing on our undersea cabling system, which remarkably, as most of you probably know, that over 90 percent of all of our information flows through these cabling systems, that we have, the three different—the varying types that we have. The organizations that sit on top that provide us those cabling capabilities, who protects the system itself, which department that may be, whether it's Homeland Security, DOJ, or Department of War? If you guys have an answer for me on that one, that would be amazing, because I can't seem to figure that one out.

How do we release our front-line operators if necessary? How do we defend against the bad actors globally that most likely know

where our cabling systems lie and how to attack them? Then I really don't really care how much redundancy we have in anything. One good one, it is kind of a showstopper.

So I threw that one to you, Mr. Bagley, but absolutely anybody on the panel, if you are educated in this in any way, please share that information with me.

Mr. BAGLEY. Thank you, Mr. Congressman, for the question. I think fundamentally, as you're noting, one of the risks posed to undersea cables comes from the physical realm and the ability to actually cut cables, to splice cables, and ultimately to redirect traffic. Right? We've seen this time and time again where adversaries have been able to do that, redirect traffic. Part of that actually goes to the network design of the internet itself, of the domain name system, and the ways in which, by design, it redirects when it reaches a dead end.

Mr. LUTTRELL. Do we have enough redundancy in place to do a redirect? Because these cables on average, what, twice a week possibly are hit and then it takes months to fix it if we can figure out who—which shoreline is going to be responsible for it.

Mr. BAGLEY. Yes, it's a great example of a cross-domain style attack in many ways that then also needs a cross-domain response. So the U.S. Navy naturally is going to own part of that, but also network operators and those who own the cables themselves, as the majority of infrastructure is owned by the private sector. So, fundamentally, a lot of what we've talked about today that I think is very important here is how to deter adversary behavior, how to make it so that their risk calculus changes when they decide that they're going to splice a cable, cut a cable. I think that's something that we should see as going well beyond just the cyber domain and thinking about all of our capabilities, including those, again, with the U.S. Navy, as far as undersea cables.

Mr. LUTTRELL. Physical security is one aspect of it. There is so many of them. When it is onshore, it is even worse considering the threat levels that exist in the metaverse that sit above our head. Putting a—I don't think globally we agree on what prosecution looks like for those that are cutting these cables, whether or not it is an accident, whether or not it is by anchor, a fishing vessel that drags there, or it is nefarious. I don't know if we can have—where we need to be because, oddly enough, what we are receiving from the private sector is very different than what we kind-of see here in Congress.

Now, where do we basically go from here is my question? Ms. Harding.

Ms. HARDING. Thank you. So one of my folks on staff is our Coast Guard fellow actually right now, who just wrote a really excellent piece on this, Joel Coito, on the undersea cables and legal prosecution options for this.

Mr. LUTTRELL. Can I get that from you guys, please?

Ms. HARDING. Absolutely, sir. I'll be sure to send it to you. I would also say, just for really precise recommendations, more repair ships so they can get back up and running quickly.

Mr. LUTTRELL. I would like to know how many.

Ms. HARDING. OK.

Mr. LUTTRELL. And what that looks like. That's information that we need to know.

Ms. HARDING. We will get you that, sir. Then I do have a lot of hope here for AI surveillance. So a lot of the ships that are accidentally, with air quotes, going after these cables are operating in very strange patterns on top of them. If you can get eyes on that target and you can identify a pattern of behavior that's anomalous, that really doesn't look much like fishing, then you can get on scene quickly and then, hopefully, deter that activity by interrupting it.

Mr. CILLUFFO. Mr. Luttrell, if I could just—we recently hosted a lengthy podcast specifically on this issue. I think you're right to underscore, if you were to compare the intelligence, without getting into anything Classified, capabilities we'd have for space, for cyber, for land, sea is—actually, we have very little visibility.

Mr. LUTTRELL. Very little. Correct.

Mr. CILLUFFO. The scale and scope and just distance is massive and the dependencies are essential. But I think here what we're really getting at, and, again, this isn't to punt on your question, but it is multi-domain. We need all the intelligence disciplines to merge and we need to invest more in undersea, there's no question.

Mr. LUTTRELL. It seems like the multi-discipline domains that live and breathe don't pay attention to everything in the middle.

Mr. CILLUFFO. Absolutely.

Mr. LUTTRELL. Because it goes under water, nobody sees it.

Mr. CILLUFFO. Absolutely right.

Mr. LUTTRELL. Mr. Chairman, I yield back. Can—

Mr. OGLES. That is fine.

Mr. LUTTRELL. OK, thank you. When we talk about the agencies and then we inject the Navy, now, I don't know if you can really move through silos very well on your side, but I tell you what, getting the Department of War to talk to Department of State or whomever, man, I was in the military, it was a very challenging thing. But since we have so much of this information that lives and breathes, do we need to increase, and I don't have a name for it, I am just kind-of making this up as I go, do we need to increase kind-of our undersea cabling fleet, as you mentioned, Ms. Harding? But I think we have two vessels, two companies that kind-of touch this. Then if you—and then of course, China and France and whomever else is really kind-of—Italy is really getting into this. Is that something that we in Congress need to talk to the Department of the Navy about? Because, honestly, the Chairman and I are really paying attention to this, but I don't think enough folks are paying attention to this.

Ms. HARDING. One hundred percent agree that not enough people are paying attention to this. Because it is such a complicated set of actors that need to be involved, and, yes, a lot of attention, a lot of focus across disciplinary effort is important. Talk to the Navy, absolutely. I think it's also about creating the incentive structures for some folks in the private sector to really invest more in the capability to protect the technology and then also to repair it.

Mr. LUTTRELL. Well, I think they would if it was so complicated to get that done because now you are dealing with the Government. Who do you think is in charge?

Ms. HARDING. Of undersea cables?

Mr. LUTTRELL. Yes. Who is a subject-matter expert?

Ms. HARDING. Inside the Government?

Mr. LUTTRELL. Or anybody.

Ms. HARDING. I know I have some at CSIS, but inside the Government, I would say that there's no one good home.

Mr. LUTTRELL. OK, thank you. Thank you, Mr. Chairman.

Mr. OGLES. You know, as fate would have it, all three of us have had these conversations about undersea cables and the vulnerabilities that they create.

But so if we will, we are getting near the end, we will pick up with you are in charge of the cyber force. What is your next step? Then once Mr. Bagley goes, we can simply go down the line one after another for kind-of closing remarks, anything that you want to emphasize that we missed or, quite frankly, that we got wrong. That is what this hearing is for. You are the subject-matter experts and we need and want to hear from you because part of my job and our job collectively is to bring this to the forefront. Because we are literally under attack and, quite frankly, I don't think enough agencies and departments are working together, that one-way street of information, and we are not fully prepared.

Mr. Cilluffo.

Mr. CILLUFFO. Chairman Ogles, thank you. God help us all if I were leading a cyber force.

But first, I think Mr. Lin captured the end-state well. I don't want to be reacting. We're always marching into the future. In essence, we've literally ceded the battlefield to our enemy. They do something, we respond. We need to be able to shape that environment. I think I mentioned suppressive fire is sort-of a tactical set of issues, adding friction into the system. I don't want to get to that point where it is already too late. If that's the time we're demonstrating our capability, game over. We've already lost to one extent or another.

So how do we do this in a proactive environment? I hate to say it, I think political will is essential here. Again, to have a deterrent, it has to be credible, it has to be consistent. If a line is crossed, you have to respond. How many more darn lines have to be crossed? I feel like we've had this discussion for a while. So I think political will, demonstrating capabilities.

Differentiating between Salt and Volt Typhoon, I'm very much where Emily is here. Salt Typhoon, it's awful, but hats off. I mean, I'm shocked there's gambling going on in the casino, to take from "Casablanca." I mean, truth is, is that's what they're doing. They're doing well. Vault Typhoon, on the other hand, is a clear line that has been crossed and there were zero consequences.

So I think, ultimately, it's bringing all instruments of national power, of which cyber is a big one. Quite honestly, I think it's unleashing some of the capabilities of not only our operators, but also our front-line owner-operator, critical infrastructure defenders.

Mr. BAGLEY. Thank you, Mr. Chairman. I think, fundamentally, you know, when we think about what's been previewed so far with the forthcoming National Cybersecurity Strategy from Director Karen Cross, and specifically PILLAR One, which focuses on this notion of changing adversary behavior, I think some core objectives that should just be baseline really are that we need to be changing

behavior so that we're diminishing the ability of the adversary to scale and diminishing the ability of the adversary to repeat. Those two basic things alone are fundamentally important when we're talking about the rate at which adversaries are adapting, the rate at which technology is evolving, and machine speed is now the speed at which we're all moving at.

So I think that in doing that, you know, as Frank was noting, I think there is a distinction, of course, between espionage used to collect information and actual cyber attacks that are attacks or that are pre-positioning for attacks. I think that's what needs to be prioritized, fundamentally prioritized, where we are changing behavior so that there are costs for attacking the United States, there are costs for attacking our allies, and that fundamentally there is a risk calculus that the adversary is going to have to take.

Mr. OGLES. Mr. Lin, closing thoughts?

Mr. LIN. Thank you, sir. Just three.

No. 1, again, I think it's absolutely critical, as you alluded to, sir, that we understand the escalation dynamics that are at play here. The escalation dynamics are such that right now, currently, there is little to no cost for our adversaries to hold our society, our country at risk, to place the digital equivalent of explosives into our critical infrastructure networks, right, in order to pre-position for war and to hold that sword over our heads. We have to change that. Playing defense simply is not enough.

No. 2, we really do have to start moving at machine speed. So while I appreciate the fact that we certainly need more talented people, we need to have the right talent pipeline going into Government, going into Cyber Command, going to DHS, going to NSA. At the end of the day, we simply cannot be throwing more people at the problem.

So that brings me to my last point, which is that we have to be smart about how we are investing in our offensive cyber capabilities. We have to make sure not just that it's resourced. So Congress passed, as you well know, sir, Congress passed a billion dollars for offensive cyber in the reconciliation bill, plus another quarter-billion dollars for artificial intelligence to be used in offensive cyber in the reconciliation bill. That's an amazing down payment. We need to make sure that resourcing is not just spent on more bodies or on legacy Government programs, but on the types of capabilities that enable our people to operate at 100X of where they are today.

Ms. HARDING. So two points.

No. 1, intel collection in the private sector. We need to take a hard look at the way we do contracting with the private sector. They have an intelligence collection network that does, in fact, rival the U.S. Government's and it is tapped, but only in a patchwork sense. This is their lifeblood, this is how they make money. So the Government does need to work with them to actually pay for that information. But there are much more efficient ways of bringing it into the system and using it across the U.S. Government for better indications and warning.

No. 2, I think this is a more strategic point. I've heard a lot today that sounds like defense and offense in the cyber realm are in opposition to each other. That's not the way to look at it. It really is both. It's a both/and. In fact, our offensive capability is severely

hamstrung by our lack of good defense. A lot of times what we see playing out in Government discussions is there's a great idea for a cyber operation and then the policy decision is, well, if we do that, then they're going to hit us back and we're weaker than they are defensively. So, in fact, we're deterring ourselves. We have to fix that defensive picture so that we can unleash on the offensive front.

Mr. CILLUFFO. Again, the challenge of going after two panelists that I agree with a hundred percent. So I'll go back with the football analogy. We actually need a head coach where both the offensive and defensive coordinators feed the playbooks into. That, I think, should be the national cyber direction. Because, ultimately, if—and to pivot to another sports analogy, if we're going to be punching, we've got to be able to absorb the punches. The reality is we have a whole lot more to lose than some of our adversaries.

The flip side is you hear a lot of people saying, oh, it's going to create escalation. I don't know what more escalation can happen before we recognize there has to be a consequence for inducing change in bad behavior.

The public-private partnership, long on nouns, short on verbs. Time we finally get to what is operational collaboration. Move beyond the information-sharing questions, which are essential. If we really want to be creative there why doesn't critical infrastructure have the ability to levy intelligence requirements? Maybe the National Intelligence Priority Framework should be open to some of our most essential critical infrastructure owner-operators. There are some creative things we can do there, but, ultimately, it can't be—if you don't have the trust that we currently do not fully have at the scale we need, if you're not in the foxhole fighting the same fight on every day, you're always going to plug-and-play in the midst of a crisis. That's not the time to be exchanging business cards. That's not the time to get to know one another. You got to do it in advance.

Mr. OGLES. Mr. Bagley.

Mr. BAGLEY. Thank you. Couldn't agree more that defense is fundamental for anything we're going to do that would be more aggressive in trying to change adversary behavior. Defense is foundational and the two should not be viewed as some sort of dichotomy that resources allocated for defense are at the expense of offense or vice versa. It's two different domains.

But defense, fundamentally, is something that should always be viewed as something that is ever-evolving. We should never think that you can make a one-time investment or choose a number that is the same number for years of investment and that that will be sufficient in protecting our Federal systems and protecting our critical infrastructure or in organizations protecting themselves around the country. So it's fundamental to note that as adversaries evolve, defenders must adapt. As new technologies are deployed, they need to be deployed with security so that they can be deployed with confidence, because if they're not, then they'll just increase the attack surface. This is fundamental as we as a country innovate with AI, adopt AI quickly, and also want to leverage the benefits from AI.

So I would implore the committee to continue the great oversight work it's doing, to think about how the U.S. Government is using these technologies, but also how the U.S. Government is increasing its own defense as it looks to change the risk calculus for adversaries.

Mr. LUTTRELL. Very well-spoken, all four of you. I would hate for all of you to walk out that door and then what you recommended to Congress never shows up again. The presentation outlined, if I was to ask all four of you, do you agree on one specific thing that you can push up to this committee, that we can help you—that might be challenging. If you are counting on Congress to write out what the internal infrastructure looks like defensively and offensively, it will fail. That is why we are—that is why you are here.

But you need to be on send while we are on receive and say, hey, through heavy negotiation, a large amount of debate, this is what we think is the baseline assessment. As we progressively move forward—because we are happy. This committee and I would assume the Majority Members of Congress understand the threat, the viable threat and risk to cyber attacks. We do. Even more so, we are getting there. You would be surprised how many people walk into our offices with a great idea that needs \$20 billion every day.

It would be nice if the collective whole of the most brilliant operators that this country has would show up, it was like, this is what we have come up with, this is the best way forward. It will flex left, right, or center. It does not have a hardcore left and right flank. You cannot do that in the digital space. But what we understand, what we know now and where we are going downstream, this is our starting point. OK, fair enough?

Thank you, Mr. Chairman.

Mr. OGLES. I want to thank you all for your testimony today. I think when you look at some of the conflict and the partisan nature that is Congress, that you see a great deal of agreement amongst the panelists, but also the Members. I think that underscores the urgency of the topic and the subject, you know, nature of the matter.

We are under attack. The war has begun and we are fighting it from multiple adversaries. We have Russia, we have malign actors, we have Iran, we have North Korea, and, of course, we have China. Let me be clear. We are the United States of America. We have been alerted. We are aware and we are watching. If I have my will, we are going on offense. We are going to strengthen our defense. There is going to be a price to pay when you incur, infringe on our borders, whether that is in the Western Hemisphere or in the cyber space.

I thank the witnesses. Members of the subcommittee may have some additional questions for the witnesses and we would ask that the witnesses to respond to these in writing. Pursuant to committee rule VII(E), the hearing record will be open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:48 a.m., the subcommittee was adjourned.]

