

UNCONSTRAINED ACTORS: ASSESSING GLOBAL CYBER THREATS TO THE HOMELAND

HEARING BEFORE THE COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES ONE HUNDRED NINETEENTH CONGRESS FIRST SESSION

JANUARY 22, 2025

Serial No. 119-1

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

60-547 PDF

WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

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

STEPHEN SIAO, *Staff Director*

HOPE GOINS, *Minority Staff Director*

SEAN CORCORAN, *Chief Clerk*

CONTENTS

	Page
STATEMENTS	
Honorable Mark E. Green, a Representative in Congress From the State of Tennessee, and Chairman, Committee on Homeland Security:	
Oral Statement	1
Prepared Statement	2
Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Oral Statement	3
Prepared Statement	5
WITNESSES	
Mr. Adam Meyers, Senior Vice President, Counter Adversary Operations, CrowdStrike:	
Oral Statement	7
Prepared Statement	9
Rear Admiral Mark Montgomery, U.S. Navy (Ret.), Senior Director, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies:	
Oral Statement	13
Prepared Statement	15
Mr. Brandon Wales, Vice President, Cybersecurity Strategy, SentinelOne:	
Oral Statement	20
Prepared Statement	22
Ms. Kemba Walden, President, Paladin Global Institute:	
Oral Statement	27
Prepared Statement	29
FOR THE RECORD	
Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:	
Statement of The Aspen Institute	70
APPENDIX	
Questions From Chairman Mark E. Green for Adam Meyers	75
Questions From Chairman Mark E. Green for Mark Montgomery	75
Question From Honorable Gabe Evans for Mark Montgomery	78
Questions From Chairman Mark E. Green for Brandon Wales	79
Question From Honorable Gabe Evans for Brandon Wales	81
Questions From Chairman Mark E. Green for Kemba Walden	81
Question From Honorable Gabe Evans for Kemba Walden	85

UNCONSTRAINED ACTORS: ASSESSING GLOBAL CYBER THREATS TO THE HOME- LAND

Wednesday, January 22, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:38 a.m., in room 310, Cannon House Office Building, Hon. Mark E. Green (Chairman of the committee) presiding.

Present: Representatives Green, McCaul, Higgins, Gimenez, Pfluger, Garbarino, Greene, Gonzales, Luttrell, Strong, Brecheen, Crane, Ogles, Biggs, Mackenzie, Thompson, Swalwell, Thanedar, Magaziner, Goldman, Ramirez, Kennedy, McIver, Johnson, Hernández, Pou, and Turner.

Chairman GREEN. The Committee on Homeland Security will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to examine the growing cyber threats to our homeland, the actors, the tactics, and the trends. Specifically, we're going to delve into the risk posed by the People's Republic of China, which has burrowed into our critical infrastructure and compromised our telecommunications networks.

We will also discuss a threat posed by our other 3 nation-state adversaries who leverage cyber space: Russia, Iran, and North Korea.

I now recognize myself for an opening statement.

Good morning, everyone. Now that we are officially organized as a committee, I'd like to welcome everybody to the 119th Congress, or as we were discussing a little earlier, the 1-1-9. We have lots of work to do to support and secure the homeland, and that is why cybersecurity is our top priority. It is why the topic of our first full committee hearing is cybersecurity.

In today's interconnected world, virtually every aspect of American life is impacted by cybersecurity; from our Nation's health care system and water supply to simple internet browsing. Cyber space is increasingly becoming a digital battlefield. America's adversaries use cyber space to undermine our sovereignty and threaten the services and infrastructure that America depends on.

The People's Republic of China, Russia, North Korea, Iran, and criminal actors weaponize cyber space to harm our Nation. They are only getting more sophisticated and, unfortunately, more aggressive. Right now, the PRC is burrowed into our infrastructure.

Let that sink in for a moment. China is pre-positioned in our infrastructure. We know it, and they have been for years.

Should we enter into a conflict with the PRC, the Chinese Communist Party is ready to shut down our essential services, our communications, our energy grid, our maritime ports, and our water systems, to name just a few. We cannot allow this situation to continue.

The American economy, our Government, the military depend upon the resilience of our networks and our infrastructure. It's past time for us to get a step ahead of the Typhoons, a list of actors that seem to grow every day. We've played defense far too long, and now it's time to go on the offensive.

To do this, we need prepared cyber professionals. I know that some of these nation-states issues go beyond what our current cyber defenders can address. This is why one of my top priorities this Congress is to pass the Cyber PIVOTT Act, which cultivates the cyber work force we need at scale. We passed it out of this committee unanimously last year, and this year we hope to get it signed into law.

We also need a coordinated whole-of-Government effort that can rapidly share information with the private sector. Since the private sector owns and operates most of the critical infrastructure in the United States, the collaboration of the organizations our witnesses represent today is essential. I look forward to hearing from our panel of witnesses about how we can improve public/private partnerships for cyber and critical infrastructure issues.

So far I've focused on one threat actor. Arguably, the one that poses the greatest risk to the United States in cyber space and beyond. However, there are many other threats that we must be prepared to address simultaneously.

For example, the Iranian Revolutionary Guard Corps has targeted our elections, notably hacking the Trump campaign in the 2024 cycle. It has also repeatedly tried to compromise U.S. water and water waste systems. The intelligence community indicates that Moscow uses cyber disruptions to influence the decisions of countries like the United States.

North Korea is a major culprit of cybersecurity and cyber crimes as well. To devise strategies to address these challenges and threats in cyber space, we must better understand them, and that's what we're doing here today.

Our witnesses will provide the insights we need to think critically about tackling current and emerging cyber threats to our homeland. All witnesses are private-sector leaders, 3 of whom bring key insights from their Government experience.

Thank you all for being here to set the scene for us as we dive into the 119th Congress. I look forward to the discussion and to a productive Congress of enhancing our cybersecurity posture.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

JANUARY 22, 2025

Good morning. Now that we are officially organized as a committee, I would like to welcome everybody to the 119th Congress.

We have a lot of work to do to support President Trump's agenda and secure the homeland. That is why cybersecurity is a top priority, and why it is the topic of our first full committee hearing.

In today's interconnected world, virtually every aspect of American life is impacted by cybersecurity. From our Nation's health care system and water supply to simple internet browsing, cyber space is increasingly becoming a digital battlefield. America's adversaries use cyber space to undermine our sovereignty and threaten the services and infrastructure that Americans depend on.

The People's Republic of China (PRC), Russia, North Korea, Iran, and criminal actors weaponize cyber space to harm our Nation. They are only getting more sophisticated—and more aggressive.

Right now, the PRC is burrowed into our infrastructure.

Let that sink in for a moment. China is pre-positioned in our infrastructure, we know it, and they have been—for years.

Should we enter into a conflict with the PRC, the Chinese Communist Party is ready to shut down our essential services—our communications, our energy grid, our maritime ports, and our water systems, to name a few.

We cannot let this happen. The American economy, Government, and military depend upon the resilience of our networks and infrastructure.

It's past time for us to get a step ahead of the Typhoons—a list of actors that seem to grow every day. We've played defense for too long, and now it's time to go on the offense.

To do this, we need prepared cyber professionals. I know that some of these nation-state issues go beyond what our current cyber defenders can address. This is why one of my top priorities this Congress is to pass my Cyber PIVOTT Act, which cultivates the cyber workforce we need at scale. We passed it out of this committee unanimously last year, and this year, we hope to get it signed into law.

We also need a coordinated, whole-of-Government effort that can rapidly share information with the private sector. Since the private sector owns and operates most of the critical infrastructure in the United States, the collaboration of the organizations our witnesses represent today is essential.

I look forward to hearing from our panel of witnesses today about how we can improve public-private partnerships for cyber and critical infrastructure issues.

So far, I've focused on one threat actor—arguably the one that poses the greatest risk to the United States in cyber space and beyond. However, there are many other threats that we must be prepared to address simultaneously.

For example, the Iranian Revolutionary Guard Corps has targeted our elections, notably hacking the Trump campaign in the 2024 cycle. It has also repeatedly tried to compromise U.S. water and wastewater systems. The intelligence community indicates that Moscow uses cyber disruptions to influence the decisions of countries like the United States. North Korea is a major culprit of cyber crimes as well.

To devise strategies to address these challenges and threats in cyber space, we must better understand them—and that's what we are doing here today.

Our witnesses will provide the insights we need to think critically about tackling current and emerging cyber threats to our homeland. All witnesses are private-sector leaders—3 of whom bring key insights from their Government experience.

Thank you all for being here to set the scene for us as we dive into the 119th Congress.

I look forward to the discussion, and to a productive Congress of enhancing our cybersecurity posture.

Chairman GREEN. I now recognize the Ranking Member for his opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman. Today marks the committee's first hearing, as you've already indicated, of the 119th Congress, and the first hearing the committee will hold during the new Trump administration. I'm encouraged by the Chairman's interest in devoting more of the committee's time to cybersecurity this Congress.

That said, I'd be remiss if I did not express concern about what we will be able to achieve. Over 6 years ago, bipartisan Members of this committee came together to support legislation, authored by then-Chairman McCaul, to establish Cybersecurity and Infrastructure Security Agency, now commonly referred to as CISA.

When he signed the bill into law, President Trump said—and I quote, “As the cyber battlespace evolve, this new agency will ensure that we confront the full range of threats from nation-states, cyber criminals, and other malicious actors, of which there are many.”

With apparent support of President Trump, Members of this committee worked together to pass legislation authored by both Democrats and Republicans to ensure CISA had the resources and authorities it needed to carry out its important Federal network and critical infrastructure mission.

Unfortunately, driven by false allegations and conspiracy theories, President Trump and many of his many Republican colleagues have soured on CISA. Less than a year ago, over 100 of them voted to cut CISA’s funding by 25 percent. Some of the loudest and most influential voices on the other side wanted to eliminate CISA entirely. So even relatively minor bills that touch CISA have been difficult to advance.

I’m hopeful that the committee’s focus on cybersecurity this Congress will help Members understand that CISA does and does—what CISA does and does not do so we can return to our bipartisan work of making the digital ecosystem safer and more secure. Bearing that in mind, we have to be clear-eyed about the enormous task ahead.

Cyber attacks from China, Russia, Iran, and cyber criminals are growing bolder and more prolific. Last year, former FBI Director Christopher Wray warned that Chinese threat actors like Volt Typhoon pose an imminent threat to the U.S. critical infrastructure because they are pre-positioning to physically wreak havoc on our critical infrastructure at a time of its choosing.

Preparing critical infrastructure owners and operators to defend and build resilience in PRC-sponsored cyber attacks requires consistent investment in CISA’s program, and that is to say nothing of its work to help private sector defend against the espionage threats posed by Salt Typhoon and Silk Typhoon or the threats posed by other adversaries.

During the 116th and 117th Congress, this committee worked on a bipartisan basis to right-size CISA’s budget so it would be well-positioned to defend Federal and critical infrastructure networks against these types of urgent threats. In fact, in 2020, the top Republican on the committee advocated that CISA should be a \$5 billion agency by 2025.

So I was troubled by DHS’s Secretary nominee’s testimony last week that she wants a smaller CISA because it’s gotten far off mission. Although it was not entirely clear what she meant by that comment, committee Democrats will oppose any effort to short-change CISA’s mission or its work force.

The Biden-Harris administration left behind a solid foundation for improving the Nation’s cybersecurity that the new administration can build upon. Its national cyber strategy put the country on a path to reduce cyber risk systematically by shifting the responsibility for security away from our constituents and on to technology manufacturers and by incentivizing the adoption and integration of better security practices.

Its Executive Orders on cybersecurity modernize the Federal Government supports to securing its own networks, to address supply chain and third-party risk, and harness the security benefits of new technologies.

For its part, CISA launched the successful State and Local Cybersecurity Grant Program, led efforts to improve the security of the technology we use through its Secure by Design program, and began to mature its operational collaboration activities through the Joint Cyber Defense Collaborative.

The new administration should not reverse course on this hard-earned progress.

Before I close, I'd also like to express my concern regarding the dismal dissemination of Government members of—I'm sorry—dismissal of non-Government members of advisory committees inside the Department, including the Cyber Safety Review Board and the CISA advisory committee.

The CSRB is in the process of investigating the Salt Typhoon hack of 9 major telecommunication companies, and it is a national security imperative that the investigation be completed expeditiously. I'm troubled with the President's attempt to stack the CSRB with lawyers because it's important work on the Salt Typhoon campaign to be delayed. The American people deserve better.

With that, I thank the witnesses for being here, and I yield back the balance of my time.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JANUARY 22, 2025

I am encouraged by the Chairman's interest in devoting more of the committee's time to cybersecurity this Congress. That said, I would be remiss if I did not express concern about what we will be able to achieve.

Over 6 years ago, bipartisan Members of this committee came together to support legislation authored by then-Chairman McCaul to establish the Cybersecurity and Infrastructure Security Agency (CISA). When he signed the bill into law, President Trump said, "As the cyber battlespace evolves this new agency will ensure that we confront the full range of threats from nation-states, cyber criminals, and other malicious actors, of which there are many."

With the apparent support of the President Trump, Members of this committee worked together to pass legislation—authored by both Democrats and Republicans—to ensure CISA had the resources and authorities it needed to carry out its critical Federal network and critical infrastructure missions.

Unfortunately, driven by false allegations and conspiracy theories, President Trump and many of my Republican colleagues have soured on CISA. Less than a year-and-a-half ago, over 100 of them voted to cut CISA's funding by 25 percent.

Some of the loudest and most influential voices on the other side want to eliminate the CISA entirely, so even relatively minor bills that touch CISA have been difficult to advance.

I am hopeful that the committee's focus on cybersecurity this Congress will help Members understand what CISA does and does not do, so we can return to our bipartisan work of making the digital ecosystem safer and more secure.

Bearing that in mind, we have to be clear-eyed about the enormous tasks ahead. Cyber attacks from China, Russia, Iran, and cyber criminals are growing bolder and more prolific.

Last year, former FBI Director Christopher Wray warned that Chinese threat actors like Volt Typhoon pose an imminent threat to U.S. critical infrastructure because they are prepositioning to "physically wreak havoc on our critical infrastructure at a time of its choosing."

Preparing critical infrastructure owners and operators to defend and build resilience to PRC-sponsored cyber attacks requires consistent investment in CISA's pro-

grams. That is to say nothing of its work to help the private sector defend against the espionage threats posed by Salt Typhoon and Silk Typhoon or the threats posed by other adversaries.

During the 116th and 117th Congress, this committee worked on a bipartisan basis to right-size CISA's budget so it would be well-positioned to defend Federal and critical infrastructure networks against these types of urgent threats.

In fact, in 2020, the top Republican on the committee advocated that CISA should be a \$5 billion agency by 2025. So, I was troubled by the DHS Secretary nominee's testimony last week that she wants a "smaller" CISA because it has "gotten far off mission." Although it was not entirely clear what she meant by that comment, Committee Democrats will oppose any effort to short-change CISA's mission or its workforce.

The Biden-Harris administration left behind a solid foundation for improving the Nation's cybersecurity that the new administration can build upon.

Its National Cyber Strategy put the country on path to reduce cyber risk systematically, by shifting the responsibility for security away from our constituents and onto the technology manufacturers and by incentivizing adoption and integration of better security practices.

Its Executive Orders on cybersecurity modernized the Federal Government's approach to securing its own networks, sought to address supply chain and third-party risk, and harness the security benefits of new technologies.

For its part, CISA launched the successful State and Local Cybersecurity Grant Program, led efforts to improve the security of the technology we use through its Secure By Design program, and began to mature its operational collaboration activities through the Joint Cyber Defense Collaborative.

The new administration should not reverse course on this hard-earned progress.

Before I close, I would also like to express my concern regarding the dismissal of the non-Government members of advisory committees inside the Department, including the Cyber Safety Review Board and the CISA Advisory Committee. The CSRB is in the process of investigating the Salt Typhoon hack of 9 major telecommunications companies, and it is a national security imperative that the investigation be completed expeditiously. I am troubled that the President's attempt to stack the CSRB with loyalists may cause its important work on the Salt Typhoon campaign to be delayed.

The American people deserve better.

Chairman GREEN. Thank you, Ranking Member.

Other Members of the committee are reminded that opening statements may be submitted for the record.

I'm pleased to have a distinguished panel of witnesses before us today and ask that our witnesses please rise and raise your right hand.

[Witnesses sworn.]

Chairman GREEN. Let the record reflect that the witnesses answered in the affirmative. Thank you. You may be seated.

I'd now like to formally introduce our witnesses.

Mr. Adam Meyers currently serves as the senior vice president of counter adversary operations at CrowdStrike where he leads the company's threat intelligence line of business. He also oversees the development and deployment of AI, machine learning, reverse engineering, and other technologies to detect suspicious and malicious cyber behavior.

Before joining CrowdStrike, Mr. Meyers was the director for cybersecurity intelligence at SRA International.

Mr. Mark Montgomery. Mr. Mark Montgomery serves as the senior director of the Center on Cyber and Technology Innovation at the Foundation of Defense of Democracies. Mr. Montgomery also directs the CSC 2.0, an initiative that works to implement the recommendations of the Congressionally-mandated Cyberspace Solarium Commission, where he serves as an executive director.

Previously, Mr. Montgomery served as policy director for the Senate Armed Services Committee. He served in the United States

Navy for 32 years as a nuclear trained surface warfare officer, retiring as a rear admiral in 2017.

Mr. Brandon Wales. Mr. Wales serves as vice president of cybersecurity strategy at SentinelOne. Before his current role, Mr. Wales served as the acting executive director of CISA, where he supervised the agency's operations and spearheaded its long-term strategy development.

Mr. Wales was also appointed senior response official, leading the domestic preparedness and response concerning the crisis between Russia and Ukraine. He spent almost 15 years at DHS in various leadership roles.

Ms. Kemba Walden. Ms. Kemba Walden serves as the president of the Paladin Global Institute, which is founded to bring the private capital perspective into technology policy. Previously she served as the acting national cyber director and was ONCD's inaugural principal deputy.

Prior to ONCD, Ms. Walden served as assistant general counsel for Microsoft's Digital Crimes Unit. She has over a decade of experience at the Department of Homeland Security.

I thank all of our witnesses for being here today, and I now recognize Mr. Meyers for 5 minutes to summarize his opening statement.

**STATEMENT OF ADAM MEYERS, SENIOR VICE PRESIDENT,
COUNTER ADVERSARY OPERATIONS, CROWDSTRIKE**

Mr. MEYERS. Chairman Green, Ranking Member Thompson, Members of the committee, thank you for the opportunity to testify today. My name is Adam Meyers, and I serve as senior vice president for counter adversary operations at CrowdStrike.

For over a decade, I've led the company's practice area, monitoring and disrupting cyber threats. Today I will share insights into the global cyber threat landscape and highlight steps we can take to strengthen our collective defenses. As a leading U.S. cybersecurity company, CrowdStrike has a unique vantage point, which gives us unparalleled visibility into adversaries' evolving tactics and allows us to see the full scope of the threats facing our Nation.

After over a decade of investing in programs to strengthen their cyber capabilities, China has matured to achieve at least parity with other world cyber powers. They now possess a sophisticated and highly effective offensive cyber capacity targeting every region and every industry vertical across the globe.

Recent campaigns demonstrate the ability to compromise large, well-resourced, and well-defended enterprises operating as providers for the rest of the technology ecosystem. One indicator of this maturation is recent Chinese operations aimed at conducting upstream or bulk collection and subsequent downstream targeting of U.S. political and national security officials.

Some notable China nexus adversaries we've observed recently include Vanguard Panda, also known as Volt Typhoon, Operator Panda, which likely overlaps with an actor elsewhere reported as Salt Typhoon, and Liminal Panda, which heavily targets telecommunications and critical infrastructure. Some campaigns are suggestive of pre-positioning capabilities which could be precursors for disruptive and destructive cyber attacks.

Over the past year, cyber nexus infusions increased 150 percent across all sectors on average compared to 2023. These increases were most significant in the financial services, media, manufacturing, and industrials and engineering sectors, which all experienced between 2- and 300 percent increases compared to previous years.

Beyond China, other threats continue to evolve. North Korea has engaged in significant financially-motivated threat activities since at least 2015. Recently, they've exploited numerous U.S. companies by pursuing remote working opportunities earning a paycheck while occasionally stealing intellectual property.

Russian nexus adversaries continue to prioritize intelligence collection against Western military, political, and diplomatic entities with their operations heavily influenced by the war in Ukraine. These actors have evolved their tactics to target mobile devices reflecting a need for battlefield intelligence.

In 2024, motivated by on-going conflicts in the Middle East, Iranian nexus adversaries continued to extensively target Israeli entities. One threat actor, Charming Kitten, collected intelligence on regional policy experts while others conducted destructive operations and information operations.

They've also begun leveraging artificial intelligence to enhance their capabilities, including vulnerability research and exploit development. From a criminal perspective, ransomware threats continue to impact all geographic regions and industries. Hacktivists, for their part, continue to grow in sophistication and also increasingly engage in for-profit e-crime in addition to pursuing social, political, and terrorist agendas.

The cyber threat landscape is complex, dynamic, and increasingly interconnected. Adversaries are constantly refining their tactics to exploit vulnerabilities across industries and sectors. To counter these threats, we must raise the cost of cyber attacks and reduce their impact. This requires investment and a collaborative effort across Government, industry, and the cybersecurity community.

I recommend that enterprises must take steps to defeat the threats I've outlined today. These include strengthening identity protection, such as through identity threat detection and response; enhancing enterprise visibility through end-point detection response; and integrating detection and telemetry data through next generation sim capabilities to enable proactive threat hunting.

The Federal Government can enhance national security by doing cybersecurity well, adopting best-in-class technologies, and more consistently disrupting adversary infrastructure. With respect to the latter, recent coordinated operations have degraded threat actor capabilities. We need to increase the tempo of these operations.

For Congress's part, it's appropriate to perform oversight to ensure Federal agencies are actively pursuing the objective outlined above, as well as ensuring resource alignment and accountability. Further, it's worth contemplating the use of tax credits, rebates, and other incentives to make best-in-class cybersecurity tools and training more accessible.

As the Federal Government takes on initiatives to modernize and create efficiencies during this period of transition, as well as review

and deprecate legacy programs and systems, there's a significant opportunity to move the needle in each of these areas.

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

[The prepared statement of Mr. Meyers follows:]

PREPARED STATEMENT OF ADAM MEYERS

JANUARY 22, 2025

Chairman Green, Ranking Member Thompson, Members of the committee, thank you for the opportunity to testify today. My name is Adam Meyers, and I serve as sr. vice president for counter adversary operations at CrowdStrike. For over a decade, I've led the company's practice area on monitoring and disrupting cyber threats. The overwhelming majority of attention during that time, and in particular over recent months, has focused on the People's Republic of China (PRC).¹ So I'll focus my remarks today on threats from that country and discuss other threats at a high level.

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, and incident response services, 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, thousands of small- and medium-sized businesses, as well as all manner of critical infrastructure entities and many foreign companies. China-nexus adversaries target each of these sectors heavily, as do threat actors affiliated with other nations.

As I've noted in a recent testimony, we started CrowdStrike in large part due to the growing impact of unchecked cyber threats—frequently from China—and the inability of existing security tools to meet this challenge. In 2011, it wasn't uncommon to see Chinese campaigns spanning scores of victims, with a multi-year duration, using extremely basic tactics, techniques, and procedures (TTPs). At that time, cybersecurity was focused on preventing the most prevalent threats, rather than the most impactful ones. Moreover, it was considered impolite, or even counter to one's economic interests, to call out this activity directly. I'm proud of the work our team—and the cybersecurity community more broadly—has done over the intervening years to change this perception. Still, there's clearly more work to be done.

At CrowdStrike, we utilize a cryptonym-based naming convention to characterize adversaries. This has become a best practice, as it permits researchers the flexibility to update attribution, account for reorganizations, and manage multiple actors with the same institutional affiliation. We assign a cryptonym once we achieve a reasonably robust confidence level in our attribution, and designate China-based adversaries as "PANDAs."² At present, we track 64 distinct PANDA adversaries, 20 of which have been recently observed, as well as a large number of other "activity clusters" with likely ties to China, but lower attribution fidelity.

KEY THREAT: PEOPLE'S REPUBLIC OF CHINA

After over a decade of investing in programs to strengthen China's cybersecurity ecosystem, China's cyber capabilities have matured to achieve at least parity with those of world cyber powers. Chinese threat actors operate complex, sophisticated, meaningfully obfuscated, and often highly-effective offensive cyber operations targeting every region and every industry vertical. Recent campaigns demonstrate the ability to compromise large, well-resourced, and well-defended enterprises operating as providers for the rest of the technology ecosystem. From an intelligence perspective, these examples highlight a growing emphasis within Chinese operations on

¹This testimony draws in part from a previous one I delivered on "Big Hacks & Big Tech: China's Cybersecurity Threat," before the U.S. Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law on November 19th, 2024. <https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/-2024-11-19pm-testimony-meyers.pdf>.

²These names generally take the form of a community- or researcher-derived codeword with some significance, followed by an animal type determined by the actor's geography or motivation. This name scheme is designed to be somewhat more descriptive than others, and can simplify communication and information sharing with government and industry counterparts, as well as assist clients' threat modeling process. For more detail, see: "Global Threat Landscape," <https://www.crowdstrike.com/adversaries/>.

“upstream” or “bulk” collection, which is notable for its efficiency, scale, and potential for impact. Other campaigns are suggestive of pre-positioning capabilities relevant for disruptive and destructive cyber attacks.

Over the past year, China-nexus intrusions increased 150 percent across all sectors on average compared to 2023. These increases were most significant in the financial services, media, manufacturing, and industrials and engineering sectors, which all experienced between 200- and 300-percent increases in observed China-nexus intrusions compared to previous years. Even among the top 3 sectors China-nexus adversaries most commonly target—Government, technology, and telecommunications—intrusion activity from China increased 50 percent in 2024 compared to 2023. Suspected China-nexus cloud intrusions increased 6 percent in 2024 across multiple commercial cloud services providers. Another marker of maturation in general is the complexity of successfully exploited systems.³

Here is a brief overview of a few recent and notable campaigns:

- Over the past year or so, VANGUARD PANDA (Volt Typhoon) drew significant attention from U.S. policy makers due to targeting critical infrastructure providers. Threat activity associated with this actor demonstrates the potential application for “preparation of the battlespace.” That is, potential use of disruptive or destructive attacks preceding or coinciding with military hostilities. For initial access, the actor targeted ubiquitous unmanaged or perimeter (edge) devices and infrastructure.⁴ These same edge devices that are integral to connecting networks to the internet provide a ripe attack surface for adversaries. Targeting these systems is fruitful because they are critical components for authentication and provide a pathway to compromise identities. These attacks are also relatively stealthy on account of reduced visibility from third-party security providers, minimal telemetry generated by system access and use, and limited forensic artifacts. Use of these techniques further limits the detection capabilities of defenders and the capacity to track adversary operations by researchers.
- At present, China-nexus adversaries heavily target telecommunications infrastructure likely in support of the intelligence collection goals of the PRC. OPERATOR PANDA⁵ is one such adversary whose attacks have been widely reported. As noted above, this activity is consistent with tradecraft that we assess is designed to facilitate bulk collection and subsequently specific targeting. In some cases, the latter appears aimed at major U.S. political and national security officials.
- Other advanced adversaries such as LIMINAL PANDA also target the telecommunications sector and demonstrate extensive knowledge of its networks, including understanding interconnections between providers and the protocols that support mobile telecommunications.⁶ Recently, this adversary compromised these networks by exploiting trust relationships between telecommunications organizations and poor security configurations, allowing them to create footholds to install multiple redundant routes of access across the affected organizations. The adversary ultimately emulated the global system for mobile communications (GSM) protocols to enable command-and-control (C2) and developed tooling to retrieve mobile subscriber information, call metadata and text messages, and facilitate data exfiltration. Actions on objectives indicated additional adversary aims of surveilling targeted individuals by gathering metadata about their cellular devices.

³China-nexus adversaries continue to increase their stealthiness and knowledge of the environments they are operating in, using novel techniques to move quickly, move laterally and escalate privileges, and remain undetected. Notably, a widely-reported 2023 breach of a major software provider demonstrated the ability to manipulate encryption systems to arbitrarily mint keys to grant the threat actors access to sensitive systems. See, “Review of the Summer 2023 Microsoft Exchange Online Intrusion,” Cyber SafetyReview Board, March 20, 2024. https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_-_Intrusion_Final_508c.pdf.

⁴This is consistent with other China-nexus adversaries increasingly moving away from the use of low-sophistication methods for initial access like spear-phishing, weaponized USBs, and credential harvesting, instead favoring specific exploitation of vulnerabilities in edge devices like firewalls, gateways, or enterprise proxies to achieve initial access.

⁵This adversary’s activity broadly aligns with previous China-nexus targeted intrusion activity tracked in industry reporting as Salt Typhoon.

⁶“Unveiling LIMINAL PANDA: A Closer Look at China’s Cyber Threats to the Telecom Sector” CrowdStrike Blog, November 19, 2024. www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/.

NORTH KOREA, RUSSIA, IRAN, AND BEYOND

As China's threat activity captures high-level attention, other threats continue to evolve. I'll mention a few high points here and can discuss at more length as appropriate.

- *North Korea*.—Amid high-profile disruptive and destructive attacks in the mid-2010's, notably the Wannacry pseudoransomware attack and blended operation targeting Sony Pictures Entertainment, North Korea has engaged in significant financially motivated threat activity since at least 2015. After 10 years of currency-generation campaigns, these operations have become a key lifeline to the regime while it is cut off from the international financial system due to sanctions. In addition to continuing to target banking and cryptocurrency targets, North Korea over the past few years has pivoted to campaigns placing malicious insiders in remote work positions. Beyond earning paychecks, these actors often attempt to steal intellectual property. In 2024, CrowdStrike Falcon OverWatch, our managed threat hunting service, responded to 304 incidents for a single prolific threat actor, FAMOUS CHOLLIMA, with nearly 40 percent of these representing insider threat operations.
- *Russia*.—While Russia-nexus adversaries continued to focus on traditional Western targets and North Atlantic Treaty Organization (NATO) member states, the war in Ukraine continued to be the primary driver of these adversaries' 2024 operations, which were focused on intelligence collection against military, political, and diplomatic entities. A need for tactical intelligence also likely forced Russian adversaries to evolve their operations to keep pace with battlefield developments in Ukraine, as exemplified by adversaries associated with the GRU (a.k.a. GU, Main Directorate of the General Staff of the Armed Forces of the Russian Federation) heavily targeting mobile devices in Ukraine.
- *Iran*.—In 2024, motivated by on-going conflicts in the Middle East, Iran-nexus adversaries continued to extensively target Israeli entities. One threat actor, CHARMING KITTEN, collected traditional intelligence on regional policy experts, while other adversaries conducted destructive operations and information operations (IO), including targeting elections. Iran-nexus actors were also among the most notable groups over the past year leveraging generative AI support in the vulnerability landscape. Iran's government aims to use Large Language Models (LLMs) in vulnerability research and exploit development, as well as to enable vulnerability-patching systems for domestic networks.
- *Rest of the World*.—While state-nexus threat activity is on the rise globally, CrowdStrike observed a concentration of activity in South Asia and the Middle East. Often, this threat activity is responsive to domestic politics and intra-regional conflict. However, many nation-states increasingly leverage cyber capabilities more broadly, including by targeting U.S. entities, for intelligence collection and intellectual property theft.

CRIMINAL AND HACKTIVIST THREATS

By volume, a meaningful share of threat activity targeting our customers comes from eCrime actors that seek to monetize malicious cyber activity. I'll share a few observations about that activity, as well as politically motivated "hacktivist" actors, which continue to proliferate.

- eCrime actors continued to represent a meaningful majority of cyber threat activity by volume in 2024. The number of publicly-named victims and CrowdStrike Intelligence's direct observations of adversarial activity demonstrate that "Big Game Hunting" ransomware actors (i.e., those that target enterprises) remain the most significant eCrime threat to organizations across all geographical regions and industries. Over the past year, these actors continued a previously-observed trend of increasingly leveraging dedicated leak sites to publicly expose data in order to extort victims. However, if there's a positive news story anywhere in the cyber domain in 2024, it's that coordinated law enforcement operations like that which targeted BITWISE SPIDER (LockBit) in mid-February and Operation Endgame⁷ in May sharply decreased the volume of key indicators we monitor like spam and bot activity, and ultimately forced adversaries to search for other initial-access methods. (I'll return to this theme in the Recommendations section, below.)

⁷"Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals," Federal Bureau of Investigation, May 30, 2024. <https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals>.

- Terrorist organizations are increasingly developing and maturing their offensive cyber operational capabilities. In 2024, CrowdStrike Intelligence attributed (that is, graduated from a cluster of linked activity to a formally-named adversary) 3 terrorist-related adversaries: 1 affiliated with Hamas, 1 with the Houthis movement in Yemen, and 1 with Lebanese Hezbollah. More broadly within the hacktivist space, we observed a potential emerging trend where a number of hacktivists were observed engaging in financially motivated eCrime in addition to threat activity furthering traditional social, political, or nationalist ideologies.

RECOMMENDATIONS

I'd like to conclude with a few recommendations for various Government entities as well as enterprises and their defenders. Our respective responsibilities differ, but across the board, our shared goal must be to raise the cost for the adversary to infiltrate our networks and reduce the impact if they do. This means we need to harden our defenses and degrade the ability of the adversary to wage successful, undetected attacks.

To this point, I've mainly focused on the threat environment and the policy landscape for confronting those threats. But I'd be remiss if I didn't at least briefly highlight some of the operational capabilities that all enterprises—whether private or public sector—can leverage to actually defend themselves. From my experience, the highest-leverage approaches are:

- Taking increasing care to defend identity across the enterprise. Compromised identities are at the core of most of the threat activity CrowdStrike has observed and responded to over the past several years. Better identity security enables a radical reduction in threats. Identity Threat Detection and Response (IDTR) tools are an important, intelligence-informed layer of the broader identity picture.
- Maintaining visibility across increasingly complex, distributed, and federated networks. Today, that requires instrumenting and monitoring traditional endpoints like laptops and desktops, network infrastructure, cloud environments, mobile and IOT devices, and increasingly, Software-as-a-Service (SaaS) applications. Such monitoring generates valuable security telemetry, designed to alert defenders to threats across each of these vectors. Endpoint Detection and Response (EDR) tools are essential to this end.
- Developing an integrated picture of IT extended environments, particularly in the face of increasing cross-domain threats (i.e., those targeting different platforms and systems). Use of technologies like Next-Generation Security Information and Event Management (NextGen SIEM) tools can help make this duty more straightforward for organizations of all sizes.

Executive Branch.—The Federal Government can enhance national security by doing cybersecurity well, adopting best-in-class technologies, and disrupting adversary infrastructure. As the Federal Government takes on initiatives to modernize and create efficiencies during this period of transition—as well as review and deprecate legacy programs and systems—there's a significant opportunity to move the needle in each of these areas.

While key U.S. Federal departments and agencies have come a long way over the past number of years on defense, there's still progress to be made. The U.S. Government itself faces among the most severe threat environments of any organization globally. Federal organizations must lead by example by ensuring Federal departments and agencies have the best tools, best training, and most informed concepts of operations for defense available. This will require appropriately resourcing and empowering Federal CIOs and CISOs. Helpfully, findings from successfully defending Federal agencies can support the development of best practices of value to other sectors, like academia, commercial enterprises, and nonprofits.⁸

Several key departments can also do more to proactively meet and defeat cyber threats. Government missions and responsibilities change over time, catalyzed by evolving opportunities, constraints, and conditions. Based on current competencies and authorities, and my observations from facilitating collaboration widely over a long period, I'll outline a few suggested focus areas. For its part, DHS, including CISA, can double down on promoting Federal cybersecurity so agencies are coordinated and operationally aligned to defeat threats. Threat actors are adept at exploiting gaps and seams, so a unified approach is essential. In recent years, the Federal

⁸For specific recommendations on improving Federal cybersecurity, see Rob Sheldon, Testimony on "Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Programs" U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection (September 19, 2023). <https://www.crowdstrike.com/wp-content/uploads/2023/11/9.19-CHS-Federal-Cyber-Testimony.pdf>.

Government has deployed 920,000 endpoint detection and response (EDR) sensors, which has helped.⁹ The task now is to layer additional mission capabilities into this infrastructure to improve vulnerability management, IT hygiene, and to enable better and more responsive managed threat hunting. CISA can also refocus on critical infrastructure cybersecurity, particularly in light of continued, consequential attacks from actors like VANGUARD PANDA and OPERATOR PANDA.

The FBI tends to lead on performing threat actor infrastructure takedowns and coordinated law enforcement actions. Efforts along these lines do take place and can be successful, such as with Operation Endgame (cited above). Still, from my vantage, over the past decade the threat environment has worsened more rapidly than our capacity to execute such operations has increased. It's now worth asking: in collaboration with international partners, what might we do to increase the tempo of disruptions by 5x? Or by 10x? It may take that scale to durably impact threat actors' operations sufficiently to raise their cost of doing business and offer meaningful relief to victims. CISA can do more to promote this mission area by providing textured, real-time insights from stakeholders, including major IT and cybersecurity providers and critical infrastructure entities, about the most pressing threats. This can inform prioritization.

The National Security Agency, Cybercommand, and other elements of the U.S. defense and intelligence enterprise have complementary roles in disrupting threat actors and their infrastructure. A full discussion is beyond the scope of this testimony but I will highlight the importance of on-going efforts to secure the Defense Industrial Base.

Legislative Branch.—For Congress' part, it's appropriate to perform oversight to ensure Federal agencies are actively pursuing the objectives outlined above as well as ensuring resource alignment and accountability. Further, to the extent that some of the defense I outlined above appear out of reach for the average small business in your State, it's appropriate to engage in a more meaningful conversation than we as a community have had to date on the use of tax credits, rebates, or other incentives to make best-in-class cybersecurity tools and training more accessible.

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

Chairman GREEN. Thank you, Mr. Meyers.

I now recognize, I guess it's Rear Admiral Montgomery—

Mr. MONTGOMERY. Yes, sir, Rear Admiral Montgomery.

Chairman GREEN [continuing]. For 5 minutes to summarize his opening statement.

STATEMENT OF REAR ADMIRAL MARK MONTGOMERY, U.S. NAVY (RET.), SENIOR DIRECTOR, CENTER ON CYBER AND TECHNOLOGY INNOVATION, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. MONTGOMERY. Thank you, Chairman Green, Ranking Member Thompson, Members of the committee for inviting me here today.

Since 9/11, every President has stated a defense of the homeland is the Nation's No. 1 priority. Despite this attention, as President Trump takes office this week, the homeland has never been less secure.

While America does remain at risk from physical attack by terrorists and even missile attacks from Russia and China, the most persistent vulnerability is a threat of cyber attack. Make no mistake, China is America's most capable and opportunistic cyber adversary.

But China is not alone. As was mentioned, Russia, Iran, North Korea, criminal actors, they all had banner years in 2024 pene-

⁹“Securing Federal Networks: Evolving to an Enterprise Approach,” Cybersecurity and Infrastructure Security Agency, January 13, 2025. <https://www.cisa.gov/news-events/news/securing-federal-networks-evolving-enterprise-approach>.

trating U.S. networks, conducting espionage, extorting ransom, stealing sensitive data.

But of greatest concern to me is China's Volt Typhoon operation which involves Chinese hackers installing malware within infrastructures. This malware lies in wait ready to disrupt and destroy U.S. systems at a time of Beijing's choosing. This campaign penetrated numerous critical infrastructures in the United States, including ports, energy systems, and water utilities. As a military planner, I used to call this operational preparation of the battlefield.

China's overarching goal in executing an operation like Volt Typhoon is to disrupt or degrade America's rail, port, and aviation systems so that the United States cannot rapidly mobilize military forces and get military equipment, personnel, and supplies to the battlefield.

Addressing these cyber vulnerabilities is going to be really challenging because the Defense Department does not control the infrastructure on which military mobilization depends. Instead, the U.S. military relies on 18 commercial ports, 70 civilian airports, and 40,000 miles of commercial rail lines. That's how we move our troops and our equipment overseas. These systems are largely owned by the private sector and local governments, and they're often maintained with insufficient levels of cyber resilience.

To make matters worse, the energy, financial services and manufacturing industries that drive economic productivity in our country, and the water, food, and health care systems that keep Americans alive, they're all equally vulnerable to this cyber attack. Both nation-states and criminals out for a quick payday take advantage.

While the private sector does own this critical infrastructure and they definitely have not done enough to invest in cybersecurity, the U.S. Government is also at fault for its poor performance as a partner to the private sector. Many of the Federal agencies that are responsible for what we call the public/private collaboration, some are even uninterested and many of them are under-resourced in the mission.

So I think, as we look for solutions, the key challenge for the United States is to restore deterrence in cyber space, making it too hard or too painful for an adversary to disrupt or exploit our networks and systems here in the United States. To do this requires both deterrence by denial and proving our defensive efforts, and deterrence by punishment, which is improving our ability to impose costs on an adversary overseas.

In my written testimony, I provide 8 recommendations, but I just want to highlight 4 of them here given the time constraints.

First, we need to secure the critical infrastructures that support military mobility. We have to address the vulnerabilities in aviation, rail, and port infrastructure and ensure that the Coast Guard, TSA, and FAA have the necessary authorizations and appropriations to execute their missions. The private-sector operators of these systems will need technical and financial assistance to combat the Chinese cyber attacks and ensure the availability of essential services at a time of crisis.

Second, we've got to prioritize assets. The United States cannot protect everything everywhere all at once. Within critical infra-

structure there are assets and entities that are more critical to U.S. national security. These assets need priority access to intelligence and incident reporting support—incident response support. Sorry. In return, the American people should expect these assets to practice a higher level of cybersecurity.

Third, we need to better utilize the National Guard to defend our critical assets. The Guard uniquely bridges military and civilian sectors, as well as Federal and State government authorities, making it ideally suited to respond to a domestic cyber threat.

The Congress should work with the Department of Defense to determine the Guard's long-term role in the cyber protection of critical infrastructure and identify any new necessary authorities, which I don't think are many, and resources, which I think will be many, to do this.

Finally, we have to recruit and develop an effective Government cyber work force. We need to hire more talent for Federal, State, and local governments. We need a program that focuses on hiring graduates from vocational schools and community colleges where students can earn skills and certifications. The Cyber PIVOTT Act from last Congress answers this challenge and should be re-attached this Congress.

In the past, the United States has had the luxury thinking about how to handle a threat from an adversary state over there in their backyard. Things are different today. To make America secure, we'll have to make the investments in cybersecurity and critical infrastructure that America has postponed for far too long.

Again, thank you for inviting me to speak, and I look forward to your questions.

[The prepared statement of Mr. Montgomery follows:]

PREPARED STATEMENT OF MARK MONTGOMERY

JANUARY 22, 2025

INTRODUCTION

Chairman Green, Ranking Member Thompson, and distinguished Members of the committee, thank you for inviting me here to testify today.

Every President since the tragic attacks of 9/11 has stated that “defense of the homeland” is the Nation's No. 1 national security mission. In his first term as President, Donald Trump approved a National Security Strategy that stated his first responsibility was “to protect the American people, the homeland, and the American way of life.”¹ As he takes office again 8 years later, the homeland has never been less secure, and America's greatest vulnerability is not a physical attack from non-state actors and terrorists, although that risk still exists. Rather, the greatest vulnerability is the threat of cyber attacks and long-range missile strikes by China and Russia—risks that undermine historical assumptions that the Atlantic and Pacific Oceans will protect America from foreign aggression.

I am confident the Armed Services Committee is looking hard into the missile defense issues, but House oversight of the protection of our national critical infrastructure from cyber attack starts here in the Committee on Homeland Security.

¹The White House, “National Security Strategy of the United States of America,” December 2017. (<https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>)

THREAT

The cyber threat is the greatest daily threat to the safety and security of American citizens and to the American way of life and the Chinese Communist Party (CCP) is America's most capable and opportunistic cyber adversary.²

Revelations over the past year have exposed the true depth of CCP cyber penetrations into U.S. critical infrastructure. These attacks should remove any doubt about either America's vulnerability or Beijing's intention to unseat the United States as the preeminent global power.

China's Volt Typhoon penetration sought to enable its hackers to lie in wait, ready to disrupt and destroy U.S. systems at the time of Beijing's choosing during a crisis.³ This campaign compromised numerous critical infrastructures, including ports, energy systems, and water utilities.⁴ As a military planner, this is what I called "operational preparation of the battlefield." Senior U.S. intelligence officials have warned that the CCP intends to activate these capabilities later during a crisis or contingency to disrupt key military logistics movements and to cause societal panic by disrupting electricity and water for the average American.

The revelations about this systematic compromise of U.S. critical infrastructure were followed later in 2024 by reports of yet another unprecedented hack by the CCP.⁵ Salt Typhoon—a different advanced persistent threat actor operated by the CCP's Ministry of State Security⁶—conducted extensive cyber espionage in the United States and other Western allies. This campaign accessed the systems of 9 U.S. telecommunications systems and internet service providers, including those used to support U.S. law enforcement and intelligence agencies in the conduct of court-authorized wiretaps.⁷ This extensive theft of data included audio recordings of telephone calls made by high-ranking U.S. Government officials.

These CCP penetrations are not a new thing. Over the past few years, there have been numerous high-profile cyber espionage campaigns conducted by the CCP against the United States, penetrating U.S. Government email systems and stealing the data that comprised many companies' intellectual property.

Meanwhile, not to be forgotten, Russia, Iran, North Korea and criminal actors all had an equally successful year in 2024, penetrating U.S. networks, conducting espionage, extorting ransoms, and stealing sensitive data.⁸ Russia's intelligence and military services have successfully conducted complex espionage attacks against the United States, such as SolarWinds,⁹ but also work closely with state-affiliated or state-abetted criminal organizations to conduct aggressive ransomware and other cyber-criminal attacks.¹⁰ North Korea is often referred to as a cyber-criminal gang masquerading as a nation-state and has specialized in ransomware and

² Cyberspace Solarium Commission, "Final Report," March 2020. (<https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report>)

³ "Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says," Federal Bureau of Investigation, April 18, 2024. (<https://www.fbi.gov/news/stories/chinese-government-poses-broad-and-unrelenting-threat-to-u-s-critical-infrastructure-fbi-director-says>).

⁴ "The CCP Cyber Threat to the American Homeland and National Security," U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, January 31, 2024. (<https://selectcommitteeontheccp.house.gov/about/events/hearing-ccp-cyber-threat-american-homeland-and-national-security>).

⁵ Sarah Krouse, Robert McMillan, and Dustin Volz, "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack," *The Wall Street Journal*, September 26, 2024. (<https://www.wsj.com/politics/national-security/china-cyber-attack-internet-providers-260bd835>).

⁶ U.S. Department of the Treasury, Press Release, "Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise," January 17, 2025. (<https://home.treasury.gov/news/press-releases/jy2792>); Greg Otto, "Malware linked to Salt Typhoon used to hack telcos around the world," *CyberScoop*, November 25, 2024. (<https://cyberscoop.com/salt-typhoon-us-telecom-hack-earth-estries-trend-micro-report>).

⁷ Martin Matishak, "US adds 9th telecom company to list of known Salt Typhoon targets," *The Record*, December 27, 2024. (<https://therecord.media/nine-us-companies-hacked-salt-typhoon-china-espionage>).

⁸ "The 2024 Year in Review: Cybersecurity, AI, and Privacy Developments," Hinckley Allen, January 9, 2025. (<https://www.jdsupra.com/legalnews/the-2024-year-in-review-cybersecurity-8353611>).

⁹ U.S. Department of the Treasury, Press Release, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," April 15, 2021. (<https://home.treasury.gov/news/press-releases/jy0127>).

¹⁰ Lily Hay Newman, "Russia's Sway Over Criminal Ransomware Gangs Is Coming Into Focus," *WIRED*, November 10, 2022. (<https://www.wired.com/story/russia-ransomware-gang-connections>); C. Todd Lopez, "In Cyber, Differentiating Between State Actors, Criminals Is a Blur," *DOD News*, May 14, 2021. (<https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur>).

cryptocurrency theft.¹¹ Iran historically fixed its cyber sights on the Iranian diaspora in the West and on Israel, but it expanded its target set to include U.S. critical infrastructure over the past 2 years.¹²

Beyond these nation-state threats lies an even more aggressive cyber criminal enterprise. The FBI received reports of \$12.5 billion in cyber crime losses in the United States in 2023, an increase of nearly 20 percent over 2022. While we know that unreported losses are much higher, the annual increase in reported crime is an accurate reflection of the growing impact of criminal activity.¹³

CONSEQUENCES

The purpose of the CCP's cyber attacks is not just to sow chaos or intimidate civilians. Chinese leaders understand that America will struggle to rapidly mobilize military forces if the rail, aviation, and port systems that move military equipment, personnel, and supplies to the battlefield are degraded or inoperable. Indeed, the success of Chinese aggression in the Taiwan Strait or Russian aggression in the Baltics, for example, could depend to a significant degree on the speed with which the United States is able to send additional military forces forward from the homeland. Last year, the U.S. intelligence community expressly warned that the CCP would "consider aggressive cyber operations against U.S. critical infrastructure and military assets" not only to deter America from taking military action in response to Chinese aggression but also specifically to "interfere with the deployment of U.S. forces."¹⁴ If adversaries can delay the mobilization and deployment of American forces from the United States, that could make it much more difficult to defeat the aggression in time.

Addressing these domestic vulnerabilities is easier said than done because the Government does not control the infrastructure on which military mobilization depends. The U.S. military primarily relies on 18 commercial seaports, about 70 civilian airports, and 40,000 miles of rail lines to move troops and equipment from fort to port and overseas. These strategic airfields, seaports, and railroads are almost wholly owned and operated by the private sector and maintained with insufficient levels of cyber resilience. For decades, many of these infrastructures have prioritized safety and physical security, adding internet-connected sensors and remote-access systems to allow real-time, cost-efficient monitoring and operations. This digitalization, however, has opened pathways for America's adversaries to penetrate and preposition malicious capabilities across the homeland.

The energy, financial services, and manufacturing industries that drive economic productivity are also privately owned and equally vulnerable to cyber attack. The lifeline systems that Americans rely on for daily life—water, food, and health care—are increasingly targeted by unscrupulous criminals out for a quick payday at the expense of the American people.

While the private sector owns the infrastructure and needs to better understand that cybersecurity is essential for core business functions, the U.S. Government has too often been a poor partner for industry.¹⁵ For more than a decade, the Federal Government has preached the importance of public-private partnerships to share cyber threat information and mitigate cyber risks. And yet, these public-private partnerships to support the resilience of America's critical infrastructures are incon-

¹¹ "The Attack on America's Future: Cyber-Enabled Economic Warfare," Eds. Samantha Ravich and Annie Fixler, Foundation for Defense of Democracies, October 28, 2022. (<https://www.fdd.org/analysis/2022/10/28/the-attack-on-americas-future-cyber-enabled-economic-warfare>).

¹² National Security Agency, Press Release, "Iranian Cyber Actors Access Critical Infrastructure Networks," October 16, 2024. (<https://www.nsa.gov/Press-Room/Press-Releases/Statements/Press-Release-View/Article/3935330/iranian-cyber-actors-access-critical-infrastructure-networks>); Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities," Revised December 18, 2024. (<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>).

¹³ Federal Bureau of Investigation, Press Release, "FBI Releases Internet Crime Report," April 4, 2024. (<https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report>); Federal Bureau of Investigation, Press Release, "FBI Releases Internet Crime Report," April 4, 2024. (<https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-releases-internet-crime-report>).

¹⁴ Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. (<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>).

¹⁵ Mary Brooks, Annie Fixler, and RADM (Ret.) Mark Montgomery, "Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure," Cyberspace Solarium Commission 2.0, June 7, 2023. (<https://cybersolarium.org/csc-2-0-reports/revising-public-private-collaboration-to-protect-u-s-critical-infrastructure>).

sistent, and the sector risk management agencies (SRMAs) responsible for this collaboration are under-resourced.¹⁶

SOLUTIONS

The 119th Congress will not be the first Congress to face this situation. As a young Naval officer, I worked at the National Security Council from 1998 to 2001 when we first tried to tackle this problem. We developed a National Infrastructure Assurance Plan in 2000, and it identified many of the same challenges I have highlighted above and some of the solutions I am listing below. Both the Clinton and Bush administrations, as well as the Congress, began to take up some of the recommendations, but all the momentum was lost in the wake of 9/11 when responding to the physical threat of terrorists became jobs 1, 2, and 3.

More recently, Congress—led by former Reps. John Katko and Jim Langevin from this committee, as well as Rep. Mike Gallagher and Senators Angus King and Ben Sasse—sought to highlight this issue, and they worked on legislation that created the Cyberspace Solarium Commission. That commission, of which I was executive director, made a series of 80 recommendations, 50 of them legislative in nature. Congress enacted nearly 80 percent of these recommendations, but some of the most important ones—the harder ones to implement—have been left unaddressed.¹⁷ And of course, as threats and conditions evolve, new recommendations have emerged as well.

The core issue is to restore deterrence in cyber space, making it too hard or too painful for an adversary to disrupt or exploit our networks and systems there. To do this requires both deterrence by denial—improving our defensive efforts—and deterrence by punishment—improving our ability to impose costs on an adversary.

Improve Our Defense

Secure the Critical Infrastructures that Support Military Mobility.—The vulnerabilities in U.S. aviation, rail, and maritime port infrastructure directly impacts America’s national security and economic productivity. As was mentioned earlier, the U.S. military primarily relies on 18 commercial seaports, about 70 civilian airports, and 40,000 miles of rail lines to move troops and equipment overseas. These assets are largely owned and operated by the private sector and are routinely assessed to have insufficient levels of cyber resilience. The SRMAs responsible for managing cyber risks to these subsectors—the U.S. Coast Guard, Transportation Security Administration, and Federal Aviation Administration—need authorizations and appropriations to fully execute their responsibilities. The private sector operators of these systems will need technical and financial assistance to combat the aggressive nature of the CCP cyber attacks and to ensure availability of essential services in a time of crisis. Congress will have to work across multiple jurisdictional issues to ensure that these efforts are synchronized for success.

Prioritize Assets.—The United States cannot protect everything, everywhere, all at once. Within critical infrastructure, there are assets and entities that are more critical to U.S. national security, economic prosperity, and public health and safety. Last April, the Biden administration rightfully tasked the Cybersecurity and Infrastructure Security Agency with working with the other sector risk management agencies to identify these systemically important entities (SIEs). The administration failed, however, to outline the benefits and burdens for companies identified as SIEs. These companies need priority access to intelligence, information, and incident response support. In return, the American people should expect them to practice a higher level of cybersecurity, which is assessed and validated by a third party or even the Government. Congress should detail the benefits and burdens of SIEs in law.

Resource Sector Risk Management Agencies for the Mission.—Congress established SRMAs as the Federal agencies responsible for collaborating with and supporting key critical infrastructure sectors. Collaboration between the Government and critical infrastructure owners and operators will not improve if SRMAs and/or Federal agencies are not sufficiently focused on this mission or resourced to undertake it. Many of these SRMAs have failed to cultivate the necessary expertise within the agency and have not invested appropriately in their staffing. One or 2 full-time equivalent workers are not sufficient to help share information, assess risk, and pro-

¹⁶RADM (Ret.) Mark Montgomery and Jiwon Ma, “We must invest in defending our critical infrastructures,” *Washington Examiner*, May 23, 2024. (<https://www.washingtonexaminer.com/opinion/3014980/we-must-invest-in-defending-our-critical-infrastructures>).

¹⁷Jiwon Ma and RADM (Ret.) Mark Montgomery, “2024 Annual Report on Implementation,” *Cyberspace Solarium Commission 2.0*, September 19, 2024. (<https://cybersolarium.org/annual-assessment/2024-annual-report-on-implementation>).

vide guidance to thousands of companies struggling with a changing cyber threat environment. Some SRMAs are barely resourced enough to maintain a website with cyber hygiene resources. Yet not all sectors need the same amount of support. Not all SRMAs need the same budgets. But all SRMAs should have sufficient resources to meet the needs of their sector. As the annual budget season begins, Congress should demand that agencies answer tough questions about their repeated failures to invest appropriate resources into helping secure critical infrastructure.

Restart Continuity of the Economy (COTE) Planning.—A core component of deterrence is our adversaries’ understanding that America can quickly recover—and strike back—if an adversary launches significant cyber attacks against us. The Federal Government needs a plan for how it will work with the private sector to restore critical economic functions rapidly. This goes beyond disaster planning for life-saving and life-safety services. What assets do we need to prioritize to restart financial flows and restore normal business operations? Congress wisely understood the importance of this complex issue and tasked the administration in the fiscal year 2021 National Defense Authorization Act with developing COTE plans. The Biden administration, however, largely failed to respond to the Congressional tasking. The effort brushed aside gaps in current Federal incident response capabilities and failed to grapple with the ways the private sector must participate in the development and implementation of the plan.¹⁸ Congress should work with the Trump administration to restart the planning process in earnest, leveraging the original legislative mandate which requires updates to the COTE plan every 3 years.

Harmonize Cybersecurity Regulations.—Critical infrastructure owners and operators are regulated by independent regulators at the Federal, State, and local level. Many of these regulators have begun imposing cybersecurity regulations, leading to a patchwork of inconsistent or redundant regulations. Private industry has repeatedly warned that duplicative regulations strain already-tight cybersecurity budgets.¹⁹ When companies demonstrate to one set of regulators that they comply with one set of cybersecurity requirements, the companies should not then have to demonstrate the same facts again to a second regulatory body. Last Congress, Sens. Peters and Lankford introduced legislation to harmonize cybersecurity regulations across the Federal Government.²⁰ Restarting efforts like this in the 119th Congress should be a priority.

Utilize the National Guard to Defend our Critical Assets.—The National Guard is the asset most likely to garner the authorities, capability, and capacity to help defend our domestic networks. As such, Congress needs to define the Guard’s cybersecurity tasking to do this. The National Guard’s unique position bridging the military and civilian sectors, as well as Federal and State government authorities, makes it ideally suited to respond to domestic cyber threats. The 54 Guard entities have the local presence and capabilities that position them well to serve as a rapid response force for cyber incidents at both the State and Federal levels. Over the years, the Guard has taken on more cybersecurity responsibilities and has built more cyber capacity. The Congress should work with the administration to determine the Guard’s long-term role in the cyber protection of critical infrastructures and identify the necessary new authorities (few, I suspect) and resources (likely many) to do this.

Recruit and Develop an Effective Government Cyber Workforce.—We need to hire, on-board, and develop cyber talent for the Federal, State, and local governments. Back in 2000, I was tasked with helping create the CyberCorps: Scholarship for Service program, which was modeled after ROTC programs: we pay for your tuition at an approved college’s cybersecurity program, and you commit to a few years of Federal service. This program has survived for 25 years and now produces 450 graduates a year for Governmental service. This program remains necessary but needs a partner program that focuses on more technical employees who hail from vocational schools and community colleges where they accrue specific skills and certifications. The Cyber PIVOTT Act from the 118th Congress will answer this exact challenge. Additionally, the Federal Government needs to do a better job on-boarding and initially guiding Federal cybersecurity workers. To that end, Sens. Mike Rounds and Jon Ossoff introduced the Federal Cyber Workforce Training Act, and Reps. Ro Khanna and Pat Fallon worked on a similar provision last Congress. When

¹⁸Mark Harvey and RADM (Ret.) Mark Montgomery, “After the Attack: A Playbook for Continuity of the Economy Planning and Implementation,” Foundation for Defense of Democracies, September 13, 2023. (<https://www.fdd.org/analysis/2023/09/13/after-the-attack>).

¹⁹Office of the National Cyber Director, “Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information,” June 2024. (<https://www.whitehouse.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf>).

²⁰David DiMolfetta, “Senate panel advances cyber regulatory harmonization bill,” NextGov, July 31, 2024. (<https://www.nextgov.com/cybersecurity/2024/07/senate-panel-advances-cyber-regulatory-harmonization-bill/398478>).

taken together, these pieces of legislation will improve the recruiting, on-boarding, and initial training of Federal cyber workers and should be pursued again in the 119th Congress.

Improve Our Offense

Enhance our Cost Imposition Capability.—Over the past 10 years, the CCP has increased the size of its operational cyber forces several-fold while the United States has remained static in its force generation capability. Despite Congressional attention and persistent efforts by U.S. Cyber Command, the U.S. military services have been unable to raise their readiness for a number of years. In addition, each service is inconsistent and sometimes ineffective in its recruiting, training, maintaining, and retaining of cyber warriors. Additionally, the size of each service's contribution to the Cyber Mission Force has not changed appreciably since the original agreements between the services and Cyber Command a decade ago despite significant changes in the cyber threat. As a result, the United States is not optimized for conflict with a Chinese adversary—which first created its own military cyber component almost a decade ago.²¹ We see the results of Beijing's investment in its cyber forces in Volt Typhoon and other attacks. The Congress needs to work with the Trump administration to fundamentally change how we generate the cyber forces which give us the ability to impose costs on our adversaries.

CONCLUSION

In the past, U.S. presidents and Congress had the luxury of thinking about how to handle the threat from adversary states “over there” in their backyard. Things are different today as the 119th Congress takes the reins. You will be looking at a variety of security challenges, but none is more serious than the cyber threats to the homeland. To make America secure again, you will have to make the investments in cybersecurity and critical infrastructure defense that America has postponed for far too long.

On behalf of the Foundation for Defense of Democracies, thank you for inviting me to testify.

Chairman GREEN. Thank you, Rear Admiral Montgomery for your testimony.

I now recognize Mr. Wales for 5 minutes to summarize his opening statement.

**STATEMENT OF BRANDON WALES, VICE PRESIDENT,
CYBERSECURITY STRATEGY, SENTINEL ONE**

Mr. WALES. Chairman Green, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to testify today on global cyber threats, a subject that I've spent nearly 2 decades focused on in Government service and in the private sector.

The past few years of publicly-acknowledged intrusions by China, Russia, Iran, North Korea, and cyber criminal organizations make clear that the United States is facing increasingly sophisticated adversaries in on-going cyber warfare. The intensity of that threat is at an all-time high, driven by a combination of increased geopolitical tensions and the rapid pace of technological change, and it shows no signs of abating.

Defenders of both the Government and the private sector are learning from each breach. However, threat actors are also evolving and innovating. Maintaining a strategic edge and building national

²¹Matt Bruzese and Peter W. Singer, “Farewell to China’s Strategic Support Force. Let’s meet its replacements,” Defense One, April 28, 2024. (<https://www.defenseone.com/ideas/2024/04/farewell-chinas-strategic-support-force-lets-meet-its-replacement/396143>); Elsa B. Kania and John K. Costello, “The Strategic Support Force and the Future of Chinese Information Operations,” The Cyber Defense Review, Spring 2018. (https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_-_Costello.pdf).

cyber resilience remains a critical challenge and will require new thinking across the public and private sector.

Among the various cyber threat actors, the People's Republic of China stands out for its persistence, breadth of operations, and capabilities, and I'll focus the remainder of my testimony here.

The threat posed by the PRC is nothing new. In 2007, they stole the plans for the F-35. In 2010, they compromised Google. In 2015, they hacked OPM. The list goes on.

As a result of these and other unprecedented attacks, Presidents Obama and Xi negotiated restrictions on cyber-enabled theft of intellectual property. However, in the wake of that 2015 agreement, the PRC retooled, they reorganized, and now they are more dangerous than ever.

According to the FBI, their hacking program is now larger than every other major nation combined. Over the past 2 years, the extent of their strategy has become alarmingly clear.

In 2023, Microsoft and the U.S. Government uncovered that Chinese actors associated with the People's Liberation Army were prepositioning on U.S. critical infrastructure preparing to launch disruptive or destructive attacks during a crisis or in the prelude to war. That summer, Chinese actors compromised Microsoft sign-in keys, granting them access to nearly anyone's email and Microsoft Exchange on-line.

Late last year, it emerged that Chinese Ministry of State Security actors had breached major U.S. communications companies. The PRC's objective is unambiguous. They are preparing for war on the networks at America's businesses, infrastructure, and Government agencies. Their goals are to prevent the United States from defending its partners and allies by disrupting our ability to project power into the Pacific and to weaken America's resolve by causing societal chaos inside the homeland.

Our response must be equally clear-eyed through a whole-of-society effort that combines Government resources, authorities, and expertise with private-sector innovation, insights, and reach, all underpinned by the support of the American people, which brings me to a series of recommendations.

First, the Federal Government should continue strengthening and centralizing critical cybersecurity capabilities within CISA, streamlining regulatory oversight of industry, and regulating smarter rather than simply more. Additionally, the Government must fully leverage its tools alongside those of our partners and allies to disrupt and deter adversaries wherever possible.

Second, business leaders, particularly our Nation's critical infrastructure, need to understand that the Government cannot save them from all threats. Cyber risks are core business risks, and, therefore, companies are ultimately responsible for their security and resilience. More importantly, if they are not already preparing for a crisis with China, they're late.

Third, the Government, industry, and the public must collectively demand more from technology, product, and service providers. We cannot secure our diverse infrastructure one system at a time. Unless the technology we depend on is secure by design, by default and in operation, we remain at the mercy of our adversaries.

Finally, we must be transparent about the sources of the cyber threats we face. Vague terms like “typhoon” or “panda” are fine for internal actor tracking, but in the broader public discourse, they obscure rather than clarify that foreign military and intelligence agencies are actively planning to attack systems critical to public health, safety, security, and economic well-being. Calling these actors by name is essential to fostering public understanding and engagement, and time is not on our side.

President Xi has instructed the PLA to be ready to militarily retake Taiwan by 2027. This means the U.S. Government, industry, and allies have only 2 years to prepare. To that end, the actions of the 119th Congress could prove among the most consequential in modern history.

I applaud the committee for prioritizing this issue first, and I look forward to your questions. Thank you.

[The prepared statement of Mr. Wales follows:]

PREPARED STATEMENT OF BRANDON WALES

JANUARY 22, 2025

Chairman Green, Ranking Member Thompson, and Members of the committee, thank you for the opportunity to testify today on global cyber threats, a subject that I have worked as the executive director of the Cybersecurity and Infrastructure Security Agency (CISA) and now as vice president of cybersecurity strategy at SentinelOne.

INTRODUCTION

The past few years of publicly-acknowledged intrusions by China, Russia, Iran, North Korea, and cyber criminal organizations make clear that the United States is facing increasingly sophisticated adversaries in on-going cyber warfare. The intensity of the threat is at an all-time high, driven by a combination of increasing geopolitical tension and the rapid pace of technological change. Defenders in the Government and the private sector are learning from each breach and adapting to offender tactics. However, threat actors are learning and innovating as well. Maintaining a strategic edge and building national cyber resilience in the face of this onslaught remains a critical challenge and will require a collaborative whole-of-Government and whole-of-industry response.

Russia

Russia’s security services are an acute and malign cyber threat, willing to take increasingly aggressive cyber and sabotage operations to undermine Western resolve in support of Ukraine. They maintain exceptionally skilled hacking teams that operate globally in support of Russian national interests, leveraging supply chain attacks and access to sensitive national critical infrastructure to hold western security interests at credible risk.

Russian security services are conducting brutal sabotage campaigns across Europe in support of their illegal war and other geopolitical goals. Intelligence collection through cyber espionage plays a role in selecting targets for disruption. In addition to conflict-related targets, Russia’s security services remain keen intelligence collectors against the U.S. Government. Political intelligence collection on personnel, the Department of Defense, and other U.S. Government elements are a high priority. They remain very skilled at combining cyber and psychological operations to interfere in elections, inflame social divisions, and undermine democratic systems across the world, and have baked these operations into their doctrine for warfare against the West.

Beyond disruption, these groups engage in economic espionage, stealing sensitive data from critical sectors to bolster Russia’s strategic interests. Ransomware gangs with tacit support from the state wreak havoc on U.S. businesses and institutions. The combined effect is deniable disruption and hybrid warfare that throws the security balance off-kilter while imposing growing costs on our society.

Russia takes a mercenary approach to its foreign policy and cyber operations. According to public reporting from the Associated Press, Russian security services are

improving their ties with the security services of the UAE.¹ Across Central Asia and Africa, Russia and the Emirates find common cause in stirring the pot in unstable countries to control gold mines and other precious resources. Their combined activities in Libya and Sudan make clear their goal to extract precious metals that help Russia blunt the impact of Western sanctions.

Iran

Iran continues to dedicate its most capable teams to attacks against Israel and Israeli targets while also actively monitoring its own dissidents internally and abroad, in some cases to target them for assassination.² Iranian attacks against Unitronics PLCs in 2023 demonstrated the intent of the Iranian regime to target Israeli companies even outside of Israel and their willingness to target industrial control systems operating critical infrastructure.³ In the lead-up to the 2024 U.S. Presidential election, the Islamic Revolutionary Guard Corps (IRGC) orchestrated a sophisticated “hack-and-leak” operation targeting President Donald Trump’s re-election campaign. Employing spear-phishing techniques, IRGC cyber operatives infiltrated campaign email accounts, exfiltrating sensitive documents, including a 271-page vetting report on then vice-Presidential candidate J.D. Vance. These stolen materials were subsequently disseminated to media outlets and individuals associated with rival political campaigns, aiming to undermine President Trump’s candidacy and sow discord within the U.S. electoral process. The IRGC’s efforts were, however, effectively neutralized by the broad unwillingness to publicize the stolen material.

North Korea

Multiple Federal indictments demonstrate how the North Koreans are trying to get their cyber operators hired into American companies so they can wreak havoc from the inside—looting companies to pay for their rapidly-advancing nuclear weapons program.⁴

Late in 2024, research by SentinelLabs showed how a web of shell companies based in China were serving as fronts for DPRK remote IT workers seeking jobs at U.S. firms.⁵ These companies were registered in China as legitimate businesses with local government through individuals in China, though it is unclear the extent to which the PRC knew of and supported these operations. Our SentinelLabs researchers tracked these registrations back to Shenyang Province in China. Reporting by CNN a decade earlier identified DPRK Military Bureau 121 operating a hotel as a front for hacking operations in the same province.⁶

Unfortunately, DPRK’s IT worker scam is still in full swing. America’s front line of defense is the H.R. department of enterprises big and small, many of which are not technically capable enough to identify discrepancies that may indicate an issue. North Korea’s effective use of mules and laptop farms create issues in detecting worker scams before these “new employees” are hired into a company.

The DPRK is also unique in that their security services are expected to turn a profit, and they do so to the tune of several billion dollars a year. These days, most of their ill-gotten gains are generated via the theft of cryptocurrencies, and many observers estimate that the North Korean government is, collectively, the largest thief of cryptocurrencies in the world. These highly fungible digital assets are then used to fund their nuclear program and evade other sanctions placed on the regime.

Cyber Criminals

Cyber criminals continue to make use of a robust ecosystem of infrastructure providers, money launderers, and tool developers to attack businesses through ransom of systems, the blackmail of leaking data, and the sale of stolen data. Ultimately, the cyber criminal ecosystem relies on 3 core factors: (1) a vulnerable and misconfigured install base here in the United States and elsewhere; (2) a cryptocurrency ecosystem outside the oversight of the traditional fiat economy by which criminals can monetize those vulnerabilities and misconfigures to extract

¹<https://apnews.com/article/intelligence-leak-russia-uae-pentagon-9941a3bb88b48d4dbb52-18649ea67325>.

²<https://www.reuters.com/world/middle-east/us-uk-taking-action-against-network-that-targeted-iranian-dissidents-us-treasury-2024-01-29/>.

³<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>.

⁴<https://www.justice.gov/opa/pr/fourteen-north-korean-nationals-indicted-carrying-out-multi-year-fraudulent-information> <https://www.justice.gov/opa/pr/justice-department-disrupts-north-korean-remote-it-worker-fraud-schemes-through-charges-and>.

⁵<https://www.sentinelone.com/labs/dprk-it-workers-a-network-of-active-front-companies-and-their-links-to-china>.

⁶www.cnn.com/2015/01/06/asia/north-korea-hackers-shenyang/index.html.

wealth from the west; and (3) a safe harbor in Russia and its sphere of influence from which the criminals can conduct their operations without fear of consequence.

The United States and allied governments have conducted effective joint operations to reduce the trust between actors, seize criminal infrastructure, and disrupt criminal networks. Still, many criminal actors persist and profit from poor cybersecurity practices in the public and private sectors. Our research and reporting will show in 2024 that the groups Akira, BlackBasta, and Play topped the metrics for frequency and profitability of their attacks. Cybersecurity companies, such as SentinelOne, are on the front line of stopping such attacks and we continue to work alongside our law enforcement partners in disrupting these operations.

China

But one threat actor, the People's Republic of China, stands out among the rest for its persistence, breadth of operations, and capabilities.

In our public conscience, the words "OPM hack, Google, Experian, Microsoft, Marriott" are anchors in our minds of China's large-scale data theft campaigns against the United States. Many now more than a decade old, we can look back on China's hacking teams and see the lack of expertise and professionalism in their old trade craft. They were noisy, easy to track, and effective.

Things have changed, though. China's hacking teams have grown significantly in size and capability over the last decade.

After Xi Jinping came into power in 2013, he quickly established the Leading Small Group on Cybersecurity and Internet Management.⁷ Within a year, he would transform that Leading Small Group into one of a handful of standing committees of the Chinese Communist Party Central Committee. It was a significant step for China and signaled Xi's personal interest in the issue.

Shortly thereafter in 2015, China revamped its cybersecurity degree requirements for universities, using the United States' own National Initiative for Cybersecurity Education as a model to replicate.

In 2016, after hearing about a project in Wuhan to establish a National Cybersecurity Talent and Innovation Base, with its own National Cybersecurity School, the CCP Central Committee on Cybersecurity and Informatization deputed it as a national project. The school graduates around 2,000 students each year that are trained in offensive and defensive cybersecurity techniques.

A year later, in 2017, China began certifying some schools as World-Class Cybersecurity Schools—a designation again meant to copy from the U.S. system. This time, the inspiration was the joint DHS–NSA Centers for Academic Excellence in Cyber Operations.

The following year in 2018, China outright banned its best vulnerability researchers from traveling abroad for 0day competitions, where they burned vulnerabilities for cash. Instead, these vulnerabilities—which China's policy community consider a "national resource"—were forced to remain in the country and surrendered to the security services at competitions like Tianfu Cup.

By 2021, China decided to do something no other government had done—they mandated the collection of software vulnerabilities, a key tool in hacking operations, be reported to the government within 48 hours of discovery by companies "doing business in China."

It should come as no surprise that we see China's hacking teams repeatedly accessing critical infrastructure, corporate trade secrets, and sensitive national security systems.

As a result of these efforts, over the past decade, China has evolved from being one of the noisiest attackers—acting without regard for being caught, while still stealing massive amounts of data—to some of the best and most stealthy hackers on the planet.

In recent years, the People's Liberation Army has tasked a group of its hackers to target American critical infrastructure and develop persistent access to those systems.

This persistent access is all too easy to procure. It will only ever take a few people, with normal laptops and the knowledge of how their targets are vulnerable, to gain and retain persistent access. Deterring this behavior may not be possible.

It is also important to note the sheer scale of Chinese malicious cyber activity is unparalleled anywhere on the globe. Each intrusion is a warning, but the vast size and pace are the true concerns.

China's view that the U.S. military is superior to the People's Liberation Army drives them to pursue asymmetric tools to weaken the United States, including

⁷ <https://www.cfr.org/blog/chinas-new-small-leading-group-cybersecurity-and-internet-management>.

cyber attacks against our critical infrastructure. The PLA believes cyber, information operations, and anti-satellite weapons are key to winning any military conflict including preventing the United States from intervening on behalf of Taiwan. So while we may be able to deter China from using these capabilities, we are not likely to deter China from preparing for conflict by prepositioning in our critical infrastructure.

Network Complexity

As adversaries grow more sophisticated, our networks have become increasingly complex. The adoption of cloud computing and expansion of remote workforces have further burdened already overextended defenders. In pursuit of constant availability, businesses have pushed technologists to deploy and maintain more tools with less down time, resulting in poor hygiene. Additionally, the rapid emergence of AI is creating vast new data repositories which carry forward these same challenges.

As a result, our networks evolved into a patchwork of interdependent services and providers, frequently built on legacy technologies predating many current defenders and defenses. These outdated foundations, central to many businesses, have become easy prey for malicious actors. Over the past decade, a surge in zero-day vulnerabilities targeting these systems has given adversaries a significant advantage. Tools and systems previously considered best-practice for security have quickly been turned against us.

Once-trusted solutions, such as VPN appliances, have become prime targets. Originally intended to protect remote workforces, these devices now represent a significant attack surface due to vulnerabilities and misconfigurations that go undetected or remain unpatched. As adversaries evolve their tactics, widely-adopted security measures can be weaponized against any organization slow to adapt.

Vendors responding to market forces have been pushed to deliver new features, to maintain a competitive edge, at the expense of comprehensive testing and secure coding practices. As a result, old classes of vulnerabilities continue to be delivered to customers, providing an avenue for threat actors to gain a foothold. This relentless pressure to innovate often backfires, putting their customers and our infrastructure at even greater risk.

Addressing these gaps calls for a collective effort by businesses, vendors, and both the public and private sectors. There is no single, fool-proof solution. As defenders strengthen their controls, attackers will evolve their methods. Emerging technologies like generative AI lower the bar for malicious actors while simultaneously providing defenders with advanced tools to detect and thwart these threats.

Driving meaningful change across the industry demands unified initiatives, such as CISA's Secure By Design, the Known Exploited Vulnerabilities catalog, Zero Trust architectures, and the NIST Cybersecurity Framework. Yet these efforts alone are insufficient. We must empower our defenders with the training and resources to counter modern threats, ensuring they possess the skills necessary to match, and surpass, those of our adversaries.

Policy Recommendations

There are steps that the Government and industry must take to weaken our adversaries, bolster U.S. cyber defenses and enhance our resilience.

First, the gravity of this moment—the continually compounding risk posed by an exploding set of cyber threat actors, highlighted by the preparation for war by the Chinese Communist Party—requires serious, straightforward conversation amongst policy makers, elected officials, business leaders, and the American public. We must call our adversaries' activities what they are—preparation for war. Accordingly, we must call them by their names, plainly, and without fanciful marketing terms that only benefit cybersecurity vendor marketing teams and the adversary themselves, by mythologizing and obfuscating. Foreign government hackers positioned to take hospitals off-line and turn off the water supply don't deserve flashy codenames, they deserve disdain and confrontation. No more typhoons or blizzards. Instead, we must speak to the American people about the provocations of the Chinese military and the Russian security services. In no other theatre of conflict do we willingly throw a veil over our adversaries and their malign activities. It must end now.

Second, to ensure that industry retains its ability to share cyber threat information without fear of liability, Congress should reauthorize the Cybersecurity Information Sharing Act of 2015, which expires later this year. This Act is an important tool to facilitate the flow of critical cyber intelligence between industry and Government, and letting it expire would be a huge step back. At the same time, the Executive branch, led by CISA, should continue to look for ways to enhance public-private operational collaboration. While CISA's Joint Cyber Defense Collaborative is a great

tool, there is more that needs to be done to ensure these efforts can achieve the scale and consistency to match the intensity of today's threats.

Third, we need a whole-of-Nation effort to engage and encourage our critical infrastructure to improve their security and enhance their systemic resilience. We are never going to stop every cyber attack so our infrastructure needs to be capable of operating in a degraded state and getting back up and running quickly. The Federal Government should be supporting our infrastructure with information, guidance, technical assistance and, in some cases, with funding. That is why Congress should reauthorize and fund the State and Local Cybersecurity Grant Program, so that our resource-constrained State and local government agencies can build and sustain minimum cybersecurity capabilities.

Fourth, the Federal Government should actively promote competition and avoid monoculture in our technology ecosystem, starting with Federal networks. Not only will this spur more innovation, but it will help create more robust systems that minimize opportunities for broad systemic failure and disruption. In part, this can be done by maintaining the momentum in recent years of investing in and centralizing cybersecurity capabilities in CISA. The establishment of CISA in 2018, a key cybersecurity win of the first Trump administration, combined with authorities granted by Congress in 2021 (e.g., persistent threat hunting on Federal networks, administrative subpoena, Joint Cyber Planning Office, etc.) and 2022 (Cyber Incident Reporting for Critical Infrastructure Act) have steadily advanced the Nation's cybersecurity capabilities. As we all recognize, however, in the modern digital economy, defenses must keep pace with the threats. Therefore, we must continually adapt and improve our defensive posture, including how we are organized, how we are resourced, how we interact across stakeholder groups, and how we respond. In that spirit, we believe elements of last week's Executive Order on cybersecurity and artificial intelligence continue much-needed forward progress on defending Federal networks, such as the accelerating persistent threat hunting and strengthening the security of internet routing. I encourage the administration and Congress alike to carefully evaluate the positive advances of the prior administration's cybersecurity executive actions and retain those that put Federal networks and the private sector alike into the best possible position to defend against constantly-evolving cyber threats.

Fifth, the U.S. Government should continue to foster our global edge in innovation in emerging and next generation technologies such as Artificial Intelligence (AI), particularly in the cybersecurity space and quantum computing. Today, AI is being more quickly integrated into cybersecurity tools, such as SentinelOne's PurpleAI, than our adversaries are able to integrate AI into their cyber weapons. In cybersecurity, speed kills, and AI-powered tools give defenders the ability to identify, investigate, and mitigate threats faster than ever before. If we want that to persist, we will need to ensure that the United States and its allies continue to lead the growth and development of AI, and that attempts to address potential AI risks don't create barriers to broader AI adoption. The PRC's enormous investments in quantum-related research and development threatens U.S. leadership as we look ahead to the emergence of quantum computing with the potential to revolutionize fields, from medicine to material science to AI, while putting much of today's encryption at risk. Congress and the Executive branch must work together to ensure that not only does the United States win the race for supremacy in quantum computing, but that American businesses and Government agencies are ready to upgrade systems to post-quantum cryptographic standards now that the National Institute of Standards and Technology (NIST) has released its first set of quantum resistant algorithms.

Sixth, the U.S. Government should aggressively pursue and counter adversary activity wherever it originates from. The takedown of LockBit in early 2024 is an excellent case study. In February of last year, Operation Cronos demonstrated to LockBit affiliates and would-be victims that the group cannot be trusted to delete data after ransoms are paid—this hit a key component of the attacker-victim relationship, trust.⁸ More recently, the operation against the Chinese actor, Twill Typhoon, by the DOJ and the FBI demonstrates the opportunities to disrupt nation-state cyber threats.

Seventh, our alliances provide tremendous value in cyber space. Takedown after takedown of ransomware operators and criminal groups make clear the value of intelligence sharing and operational coordination across allied nations. More importantly, when attempting to address the intrusions by nation-state actors, such as China and Russia, intelligence-sharing agreements between like-minded nations, in-

⁸ <https://globalinitiative.net/analysis/the-lockbit-takedown-law-enforcement-trolls-ransomware-gang/>.

formation sharing on adversary tactics, unified messaging and joint action are all critical in preparing for, stopping, and countering adversary action.

CONCLUSION

Our Nation continues to face unprecedented risks in cyber space and our success in addressing this challenge is dependent on how effectively the Government, industry, and allies work together. No one organization or company can do this on their own. We need the unique expertise, skills, and authorities resident across these communities, and time is not on our side. I applaud the committee for making this subject its first hearing of the 119th Congress, and I look forward to working with the committee in the months ahead.

Chairman GREEN. Thank you, Mr. Wales.

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

STATEMENT OF KEMBA WALDEN, PRESIDENT, PALADIN GLOBAL INSTITUTE

Ms. WALDEN. Chairman Green, Ranking Member Thompson, distinguished Members of the committee, thank you for inviting me to testify today on this important topic.

I'm Kemba Walden, president of the Paladin Global Institute and co-chair of the Aspen Digital U.S. Cybersecurity Group. I'm here today in my personal capacity drawing from my experience as former acting national cyber director and my roles at Microsoft and at the Department of Homeland Security.

The last year—4 years have seen new sophisticated cyber threats, each of which has highlighted why cyber remains a significant source of human-caused risk to our homeland. We saw the 2020 Russian attack on the SolarWinds Orion platform, and then the 2021 ransomware attack against Colonial Pipeline, and then in 2022 the first shots fired in Russia's unprovoked war of aggression in Ukraine were from a cyber attack targeting an American satellite communications company.

Each of these incidents represents a clear national security threat in their own right, and I haven't even mentioned the Microsoft Exchange Server debacle, Log4j, or the billions of dollars spent in the aftermath of Change Healthcare. Yet, there are 2 campaigns in the past 4 years that I hope the committee will focus its attention on.

The first is the recently-uncovered targeting of our Nation's critical infrastructure by the People's Republic of China. This activity dubbed Volt Typhoon represents a step change in the PRC's cyber operational capability, demonstrating their willingness to pre-position in our critical infrastructure in preparation for a future conflict.

Second, we've now witnessed the PRC snooping on our telecommunications networks. Salt Typhoon shows the PRC investments are paying off in truly a scary fashion, as they have accessed the beating heart of the internet itself.

I raise these 2 examples to highlight the stakes we face. The PRC's capabilities are rapidly improving, and we have seen from their behavior that they are ready to use cyber tools to attack our critical infrastructure. But despite these threats, there are key steps that Congress and the new administration can take to increase our resilience and improve the Nation's cybersecurity posture.

We must strengthen national cybersecurity by clarifying roles and responsibilities of the private sector and Government, upscaling our collective work force, and embracing technological innovation. On the first, the roles and responsibilities front, there are 3 legislative actions that I would offer as low-hanging fruit for you to consider.

The Cybersecurity Information Sharing Act of 2015 expires in September. This committee must take action to reauthorize that legislation to ensure we do not see hard-won progress lost to Congressional inaction.

I also urge the committee to further clarify liability protections related to the defensive measures to allow for the most proactive defensive approach possible. Regulatory harmonization is an enormous challenge that places an untenable burden on business while harming our cybersecurity.

Last Congress, Senator Peters, Senator Lankford, and Congressman Higgins introduced legislation to help bring coherence to the multitude of Federal regulatory approaches by empowering the national cyber director, and Congress should move swiftly to reintroduce and advance this important bill.

This committee should also work to codify the Cyber Safety Review Board, or CSRB, which helps to understand the root cause of cyber incidents to keep us from making the same mistakes over and over.

I hope you will consider strengthening the board by making it full-time, independent, and nonpartisan with its own administrative subpoena power. Of course, all the policies in the world are meaningless without the work force implementing them.

While there are several successful programs that are helping to put a dent in the hundreds of thousands of unfilled cyber jobs we have in this country, there is absolutely more we can do.

To remain sustainable, Congress should expand CISA's current cyber work force programs, increase the number of internships and apprenticeships available to qualifying students with or without college degrees, and provide incentives for cyber professionals to work at under-resourced targets, like hospitals and water systems.

Finally, I urge you to embrace technology, including from venture-backed companies that are truly at the cutting edge and allow it to be part of the solution. Supporting the use of artificial intelligence, for example, for threat detection and response can help neutralize sophisticated cyber threats more efficiently.

Distinguishing between our digital presence, knowing who is who and that you are you is of paramount importance to cybersecurity for the—the Federal Government must update its digital identity guidelines to prevent unauthorized access, phishing, and email-based attacks and decrease cyber fraud of public benefit programs.

In conclusion, the global cyber threat landscape requires a coordinated proactive approach combining legislative action, technological innovation, and operational collaboration. Acting together, we can protect our national security interests while fostering innovation and economic growth.

Thank you again for the opportunity to appear before you, and I look forward to your questions.

[The prepared statement of Ms. Walden follows:]

PREPARED STATEMENT OF KEMBA WALDEN

JANUARY 22, 2025

Chairman Green, Ranking Member Thompson, distinguished Members of the subcommittee, my name is Kemba Walden, and I am the president of Paladin Global Institute (Paladin), a think tank committed to ensuring that secure critical infrastructure and the safety of people on-line remain core to sustainable technological innovation. I also serve as a co-chair of Aspen Institute's U.S. Cybersecurity Group, which published cybersecurity policy recommendations for the new administration, some of which are reproduced below, based on the collective experience and expertise that membership gained over decades of experience in the public and private sectors.

Prior to Paladin, I served as the acting national cyber director and the first principal deputy national cyber director in the Office of the National Cyber Director in the Executive Office of the President. Before that, I was an assistant general counsel in Microsoft's Digital Crimes Unit (DCU), where I led the Ransomware Analysis and Disruption Program. I also spent a decade in Government service at the U.S. Department of Homeland Security (DHS) in several attorney roles, specifically as the DHS lead for "Team Telecom," the lead attorney for the DHS representative to the Committee on Foreign Investment in the United States (CFIUS) and then as a cybersecurity attorney for the Cybersecurity and Infrastructure Security Agency (CISA), and its predecessor.

Over the course of my career, I've witnessed the evolution of global cyber threats, new approaches to exploiting vulnerabilities in technology, and our responses to them. There are 3 types of cyber threats—nation-state actors, criminals, and insider threats. And there are 2 evolving types of vulnerabilities—the pace of technological advancement, and the status quo of business processes. The impact of these threats and the creativity and sophistication with which malicious are exploiting vulnerabilities is considerable.

The world is in a state of flux. The risks are too high to continue to take a tactical approach to responding to these threats individually. Faced with this strategic context, we must continue to pursue a more resilient and defensible infrastructure that is aligned with our values. A sustainable and successful effort against these threats will require a whole-of-Government strategy executed in close partnership with the private sector, our allies, and international partners.

Over time, we've matured our governance and developed strategy, but there's much more to do. In this testimony, I first describe 3 types of global threats and 2 pernicious vulnerabilities—and second, I offer governance, skilling, and technological solutions to mitigate the resulting risks.

In this testimony, I will leverage the expertise gained through the work of Paladin Global Institute, its insight into various markets, and my experience through Aspen Digital and previous roles, to provide an overview of the threat landscape and provide recommendations I believe this subcommittee may find relevant as it continues to consider responses to these global cyber threats. Paladin Global Institute leverages its global reach and deep bench of cutting-edge thought leaders and policy experts to protect global critical infrastructure. Paladin encourages both (1) operational opportunities to mitigate cyber threats and vulnerabilities and (2) policy solutions for sustainable cybersecurity and cyber safety improvements.

A. THE EVOLVING LANDSCAPE OF GLOBAL CYBER THREATS AND VULNERABILITIES

1. *Nation-State Actors*

As the world bears witness to the transition to a new administration and a new Congress, our adversaries are considering exploiting vulnerabilities in the seams created by the transfer of power. It is in these transitions where pernicious threats thrive, and vulnerabilities loom largest. To advance their own geopolitical standing in the world and to impact the balance of alliances, nation-state threat actors aim to strike when the United States is at its most vulnerable. These threat actors use diverse methods to achieve their geopolitical aims, but they share common goals. They each need for the United States to appear weak and off-balance, and they've learned that there's opportunity during times of transition.

These threats are coalescing around common goals. This month, Russia signed a treaty with Iran to expand economic and security ties between the 2 countries. Last year, North Korea also signed an agreement with Russia to provide military assistance in times of war. In 2022, China and Russia announced a formal partnership announcing that there are "no limits" to areas of cooperation between the 2 countries. These reported alliances inform the dynamic nature of global cyber threats.

Russia

Russia uses cyber operations as a foreign policy lever to shape other countries' decisions, focusing on cyber operations to gain advantage in the Ukrainian war and the region, but continuing to target critical infrastructure in the United States. When the Biden administration was transitioning into office, it did so in the wake of the Russian state-sponsored breach of the SolarWinds Orion platform. This supply chain attack was novel in its approach, and unprecedented in its reach. Russian-backed cyber criminals then breached Colonial Pipeline and held it for ransom. The world then watched the subsequent run on gasoline across the East Coast of America and learned that cyber has power in the real world. Russia's Federal Security Service has long-standing ties to national cyber criminals and indigenous hacktivist communities. Because of their relationship with the government, the government tacitly permits criminals to operate, shielding them from U.S. law enforcement.

The People's Republic of China (PRC)

As noted in The Office of the Director of National Intelligence's 2024 Annual Threat Assessment, "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks." As the People's Republic of China (PRC) seeks annexation of Taiwan, with U.S. Adm. John Aquilino, head of U.S. Indo-Pacific Command, noting "all indications" point to the Chinese military being ready for a potential invasion of Taiwan by 2027, the PRC has moved to prepare the battle space. Long gone is a China simply focused on IP theft; we've now witnessed China snooping on telecommunications networks (i.e., Salt Typhoon) and prepositioning in U.S. critical infrastructure to enable disruption operations in preparation for a future military conflict with the United States (i.e. Volt Typhoon).

The most recent revelations about China's massive cyber attacks on U.S. critical infrastructure and telecommunications networks demonstrate the increased sophistication of PRC threat actors, and the expansion from espionage to potential disruption or destruction activities. Although the PRC threat actors used to be known for "smash and grab" cyber intrusion, they've moved to a new era of stealth cyber intrusion, with the PRC exploiting legitimate privileges in private-sector systems not only for espionage, but more importantly to hold our critical infrastructure at risk. Through an operation, named Volt Typhoon, we discovered that the PRC were "living off the land" in our infrastructure to evade our detection technologies. Over time, the PRC gained sophisticated knowledge not only of our technology but of the governance structure through which we secure that technology, forming creative opportunities for exploiting new vulnerabilities.

One additional known PRC penetration strategy is through PRC investment in U.S. critical infrastructure. Working often through creative investment vehicles, the PRC took a strategic approach to eventually holding our infrastructure at risk while the United States took a tactical approach to blocking transactions that raised national security concerns. As your committee found in an investigation, this includes investment in the maritime industry, with 2 PRC state-owned enterprises controlling portions of 5 U.S. ports. Notably, the PRC is outpacing most national investments in emerging technologies. According to some reports, the global investment in quantum technology is over \$40 billion, with the PRC driving approximately \$15 billion in investments whereas the United States is investing just under \$5 billion.

As early as 2012, the House Committee on Intelligence warned that "the United States should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies" and further recommended that "Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure." In response, at the direction of Congress, the Federal Communications Commission established the Supply Chain Reimbursement Program to reimburse small providers of advanced communications services for expenses related to the removal and replacement of communication equipment and services provided by Huawei or ZTE. More work remains to be done to remove Chinese equipment from our critical infrastructure, including TP-Link consumer routers in the United States which have been used to launch cyber attacks via a Chinese hacking entity that maintains thousands of compromised TP-Link routers. The fact that TP-Link is dumping routers in the U.S. market below a profitable point has enabled them to move from 8 percent of the market to 60 percent in only a few short years. The PRC is playing the long game for an operational and strategic advantage.

Iran

Iran seeks dominance in the Middle East and conducts influence operation in the United States to include targeting U.S. elections. Just this summer Iran's Revolutionary Guard Corps-affiliated cyber actors targeted the Trump campaign, in efforts to erode confidence in the U.S. electoral process ahead of the November Presidential election. In addition, we have seen Iran-based cyber actors enabling ransomware attacks and using brute force to compromise U.S. health care and other critical infrastructure providers.

Democratic People's Republic of Korea (DPRK, a.k.a. North Korea)

The Democratic People's Republic of Korea (DPRK) seeks the survival of the dynasty and to "reunify" the Korean peninsula under their terms and vision. Cyber operations are a main source of funding for the Government which get around U.S. and international financial sanctions. In the earliest days of the Biden administration, as blockchain technology was maturing and the virtual currency system built upon that technology were gaining in popularity, the DPRK found opportunities to exploit them for financial gain. Initially, the DPRK used ransomware to obtain virtual currency, but they later learned that exploiting vulnerabilities in blockchain technology and stealing virtual currency from cryptocurrency exchanges is far less expensive. We have also seen an uptick in DPRK targeting of critical infrastructure to steal technical information and IP to further its nuclear ambitions.

2. Cybercriminals and Fraudsters

The proliferation of cyber crime presents an escalating threat to our national and economic security. As reported by the FBI, criminal activities ranging from business email compromise, investment scams, ransomware, and fraud resulted in potential losses of over \$12 billion in 2023. The General Accountability Office estimates that cyber fraud costs the U.S. Federal Government between \$223 billion and \$521 billion every year. Organized criminal groups have developed sophisticated ransomware operations impacting the operations and availability of critical infrastructure, including health care facilities, and Government institutions. Of particular concern are the emerging trends of criminal networks recruiting and exploiting minors for cyber operations, creating both a security and societal challenge, and the proliferation of ransomware as a service, allowing less sophisticated cyber criminals to launch attacks at a lower cost. An insidious through line across many of these nation-states and cyber criminals is the abuse of network access and privilege, with threat actors stealing credentials through phishing attacks, social engineering, and malware.

Ransomware has evolved into a highly lucrative business model, with threat actors using advanced intelligence collection to shape ransom demands. Once criminal actors break into a network, they may access and study their target's financial documents and insurance policies, and research the penalties associated with data breach laws, to better inform their eventual ransom demand and negotiating position. Leveraging this significant intelligence gathered on victim companies, the criminal actors then launch their ransomware attacks, identifying what they regard as an "optimal" ransom amount. These criminal actors extort money from their victims, not only to unlock systems but also to prevent public disclosure, making significant money from data theft and double extortion, and deploying thousands of instances of malware across thousands of victims.

As cyber crime has evolved to more enterprise-like operations involving multiple players, countering these efforts requires a multi-stakeholder and global approach. The private sector and the U.S. Government have engaged in and experimented with technical and legal models, globally, to disrupt and dismantle cyber crime infrastructure. Efforts to date illustrate that a collaborative multi-stakeholder approach—sharing actionable information and leveraging the combined capabilities of the private sector and the Government—yields the best opportunity to disrupt cyber crime quickly and at scale.

Paladin's direct experience with technology companies engaging in public-private partnerships has shown how potent collaboration can be. One technology company's facilitation of many hundreds of FBI victim notifications had an impact far wider than just protecting the notified victims. In one engagement, the company intercepted an attack against an IT provider with over 600 large financial institution customers. The threat actor was planning to sell access to a ransomware affiliate who would then attempt to encrypt the IT Provider's customer networks, creating a catastrophic impact on not just the victim's business, but its many customers. Public-private partnerships, when scaled up as in this case, can disrupt the criminal supply chain, thereby making it more difficult for ransomware affiliates to successfully find and attack victims.

The cyber crime ecosystem is dynamic and massive, but the Federal Government has done incredible work to hold these malicious actors accountable. The National Cyber Investigative Joint Task Force, law enforcement agencies, U.S. Cyber Command, the National Security Agency, and other elements of the intelligence community have led multiple initiatives to increase the speed and scale of disruption operations, coordinating joint, sequenced disruption campaigns with international partners. Sustained efforts, and investments, in these programs will continue to defend the Nation and our critical infrastructure from ransomware threats.

3. Insider Threats

The increasing globalization of the job market, rise of remote work, and need for highly specialized skilled workers provides global adversaries—specifically the DPRK and the PRC—an opportunity to creatively target U.S. companies’ sensitive intellectual property (IP), high-tech research and development (R&D), and financial assets. Information Technology (IT) workers often have privileged access to systems. So, while today they may just be a source of hard currency (and occasional R&D), they could use their positions of trust to conduct more conventional cyber operations.

Since at least 2022, information technology (IT) workers from the DPRK have been fraudulently obtaining remote employment at unwitting companies in the United States, including at Fortune 500 companies across a variety of industries. DPRK threat actors use U.S.-based job search sites to seek employment with U.S. companies and use stolen U.S. citizens identities to gain employment. This scheme often requires the assistance of other U.S. individuals as facilitators to help the DPRK workers appear to be in the United States and move money and IP out of the United States. These works, some of whom live in China and Russia, provide a critical revenue stream that helps fund DPRK economic and security priorities and helps the DPRK gain access to sensitive IP and R&D. These fraudulent employees put U.S. companies at risk of violating U.S. and international sanctions and put IP and sensitive data at risk.

Similarly, Chinese intelligence services abuse U.S. student and work visas to gain access to critical technology at U.S. companies and universities that require highly technical and skilled workers to fill critical technology roles. For those U.S.-trained Chinese nationals who otherwise cannot lawfully stay in the United States upon completion of their studies, the PRC benefits from the talent and skills and knowledge of those students when they return. Intellectual property theft from U.S.-employed or -trained Chinese nationals poses a significant risk to the private sector and academia, particularly amongst the defense sector and emerging dual-use civil-military technologies, such as Artificial Intelligence (AI). In fact, approximately 60 percent of all FBI trade secret theft cases involve a nexus to the PRC. For example:

- In 2018, Chinese state intelligence actors used a U.S.-based job search site to target and clandestinely recruit a former U.S. intelligence community employee at Boston University, assessed U.S. military websites, and exfiltrated sensitive documents and information back to China.
- From 2022 to 2024, U.S.-based Chinese national employee exfiltrated sensitive company proprietary AI technology and research to 2 PRC-based startups.
- In 2019, a U.S.-based Chinese national pleaded guilty to stealing over \$1 billion in petroleum research and development from 2017 to 2018.
- In 2020, People’s Liberation Army Lieutenant Yangqing Ye falsely posed as a student to enter the United States on a J-1 visa. While posing as a student, Ye conducted biomedical research.

4. Technological Acceleration

The rapid pace of technological advancement, while offering tremendous opportunities, also presents significant security challenges. As innovations in fields like AI, quantum computing, and biotechnology emerge at an unprecedented rate, they bring both exciting possibilities and potential vulnerabilities. It is in the seams where innovative technologies are integrated into legacy IT systems, that our adversaries find exploitable opportunities.

As stated in the 2024 Report on the Cybersecurity Posture of the United States and 2024 Annual Threat Assessment, these technological advancements can enhance our capabilities in various sectors, from health care to transportation, but they also create new attack vectors for malicious actors. The interconnectedness of our digital infrastructure means that a single vulnerability can have far-reaching consequences, making it crucial to stay ahead of potential threats.

We must shift from reactive to proactive security postures to address emerging threats from quantum computing, AI, and other transformative technologies. This paradigm shift requires a fundamental change in how we approach security, moving

away from simply responding to threats as they occur to anticipating and mitigating risks before they materialize. For instance, the development of quantum-resistant cryptography is essential to protect sensitive data from future quantum computing attacks.

Similarly, leveraging artificial intelligence and machine learning for threat detection and response can help identify and neutralize sophisticated cyber threats more efficiently. Proactive security measures also involve continuous monitoring, threat intelligence sharing, and regular security assessments to identify and address potential vulnerabilities before they can be exploited.

This requires forward-thinking policies and adaptive security frameworks and long-term investments in technology. The U.S. Government and private sector need to develop comprehensive strategies that not only address current security challenges but also anticipate future threats. These policies should be flexible enough to evolve with the rapidly-changing technological landscape. Adaptive security frameworks should incorporate principles of resilience, allowing systems to detect, respond to, and recover from security incidents quickly.

Capital investments in cutting-edge security technologies and innovation hubs focused on cybersecurity research and development are crucial components of this approach. Additionally, streamlined procurement processes can ensure that organizations can quickly adopt and implement the latest security solutions. By fostering collaboration between the public and private sectors, as well as academia, we can create a robust ecosystem of innovation and security that is better equipped to face the challenges of technological acceleration.

5. *Status Quo Business Processes*

Supply Chain Attacks.—Cyber threat actors’ exploitation of critical vendors has highlighted the need for robust cyber supply chain risk management and vendor vetting. From the SolarWinds Orion platform breach in 2020 to Okta in 2023, the concentration of risk in and across supply chains demands constant attention. Third party risk management is a critical part of supply chain security, and I was encouraged to see that the National Institute of Standards and Technology (NIST) added cyber supply chain risk management across several publications in the last 4 years, including the Cybersecurity Framework 2.0.

Investments, Mergers & Acquisition.—Cybersecurity challenges are commutative and can transfer during mergers and acquisitions. The United States’ historical openness to foreign investment has also been exploited by competitors. The National Counterintelligence and Security Center (NCSC) has issued guidance warning start-ups that foreign threat actors could invest in their companies to “harm U.S. economic and national security interests.” The FBI is reportedly investigating Hone Capital, which launched in 2015 with an initial investment of \$115 million from a Chinese private equity group and has invested in over 350 U.S. tech start-ups. The investment has allegedly resulted in the transferring of trade secrets and intellectual property back to Beijing.

It is imperative to invest capital in technologies that adhere to U.S. law, conform to U.S. sanctions, and are not subject to the jurisdiction of adversarial nations before they go to markets. These trusted capital principles promote security, trust, safety, and national security before products go to market. When the company is secure by design and intent, the digital ecosystem it then joins is, too.

This complex and multi-actor threat demands of us sustaining investments in innovative, intrepid, and industry-led solutions.

B. POLICY RECOMMENDATIONS

We must strengthen national cybersecurity by prioritizing security across all lines of efforts by clarifying roles and responsibilities of the private sector and Government, upskilling our collective workforce, and embracing technological innovation that will enhance the resilience of our infrastructure against cyber attacks. These strategic investments will yield greater returns in our security.

1. *Policy Solutions to Clarify Roles and Responsibilities*

Continue Building Mechanisms to Measure Progress.—Government efficiency depends on good data and clear-eyed analysis. We cannot understand what works without data. We need a repository of data in this area to know what cybersecurity regulations and programs to keep and what to cut.

Clarify Lawful Proactive Solutions for Industry and Improve the Cybersecurity and Information Sharing Act of 2015 5 U.S.C. §§ 1501–1510.—The current state of U.S. infrastructure vulnerability is unacceptable. Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the

same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies, and terrorists should be hunted jointly with key private-sector actors. Efforts to “defend forward” must be continued in conjunction with providing resources and assistance to critical, often overlooked entities such as small businesses and rural communities. Further, we must leverage the United States’ unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

Industry cannot defend the infrastructure the Nation relies upon without the assistance of the U.S. Government and its allies. We cannot expect industry alone to defeat nation-state actors. The Cybersecurity Information Sharing Act of 2015 was a good start to encouraging better collaboration between the private sector and Government. Congress authorized certain protections to industry if they shared cyber threat indicators and defensive measures within industry and with the Government for cybersecurity purposes. As the law is up for renewal, Congress should consider more precision in defining defensive measures (5 U.S.C. § 650) so that the lines between proactive defense and “hacking back” are clearer. Most importantly, this committee must take action to reauthorize CISA 2015 before it lapses in September to ensure we do not see hard-won progress lost to Congressional inaction.

Prioritize Cybersecurity Regulatory Alignment and Streamlining.—Regulatory harmonization is another key issue for the committee to consider. Under my leadership at ONCD—and in alignment with the National Cybersecurity Strategy Implementation Plan—we put out an extensive request for information to the private sector to understand their challenges with overlapping regulatory regimes. What we heard was startling. Businesses of all sizes and from 11 of the 16 critical infrastructure sectors reported that the compliance burden was hampering their cybersecurity programs. One industry group reported that CISOs were spending 30 to 50 percent of their time focused on compliance. This is not only a drain on our economy—it actually leaves us less secure, by keeping cyber operators filling out paperwork instead of defending systems.

Last Congress, Senator Peters, Senator Lankford, and Congressman Higgins introduced legislation to help bring coherence to the multitude of Federal regulatory approaches. The bill would have empowered the National Cyber Director to convene all of the relevant parties, including independent regulators, to develop a set of cross-sector minimum requirements that would have reciprocity baked in. A business that operates in multiple sectors—or that is in the supply chain of many regulated entities—would only need to show they met the baseline once. I am very confident this approach will both meaningfully improve our cybersecurity posture and reduce compliance costs, and I hope Congress will continue last year’s momentum and move swiftly to enact this legislation. In this post-Chevron era, the incoming administration’s work with Congressional leadership will be critical.

Of course, cybersecurity is a global challenge, and the regulatory landscape is changing swiftly internationally as well. Late last year, dozens of multinational chief information security officers sent a letter to senior leaders from the Organization for Economic Co-operation and Development (OECD) countries urging them to add regulatory harmonization to the OECD’s digital agenda. This builds on work former DHS Secretary Mayorkas did earlier in 2024, in partnership with the European Commission, to catalog overlapping incident reporting regimes. I urge this committee to champion international regulatory harmonization work, including through venues like the OECD, to ensure a level playing field across the markets of our allies and partners—and to achieve our shared interest in protecting our critical infrastructure from adversary nations and cyber criminals.

Support and Instantiate the Cyber Safety Review Board (CSRB).—The Cyber Safety Review Board has played a critical role in fostering transparency and accountability and driving improvements across Federal agencies and critical infrastructure providers. This committee should consider how to codify and strengthen the CSRB’s role in providing a mechanism to learn lessons from past incidents and strengthen our Nation’s cyber defenses. Steps to strengthen the CSRB include making a full-time, independent, non-partisan board, with a full-time technical staff and administrative subpoena power. Independence will enhance the credibility of CSRB’s investigations and advice.

2. Policy Solutions for Investing in a Skilled Workforce to Combat Cyber Threats

Expand support for the Federal Cyber Scholarship-for-Service Program.—5 U.S.C § 7442 and the National Center of Academic Excellence Program in Cybersecurity.—The integration of emerging technologies into legacy systems, the maintenance of those systems, and the security of technology requires a well-skilled workforce in the private and public sectors. Over the last several years, Congress has proffered

positive legislation to improve our workforce. As succinctly described in the National Cyber Workforce and Education Strategy, Federal programs in cyber workforce and education reinforced the importance of sustained Federal investments by establishing a foundation for cyber workforce and education program development to provide a pipeline of qualified cyber talent. These legislative efforts include the National Center of Academic Excellence program in Cybersecurity led by the National Security Agency (NSA); the CyberCorps®: Scholarship for Service (SFS) program, led by the National Science Foundation (NSF) in coordination with the Office of Personnel Management and the Department of Homeland Security; the Department of Defense Cyber Service Academy; the Cybersecurity Education and Training Assistance Program led by the Cybersecurity and Infrastructure Security Agency; and the National Initiative for Cybersecurity Education led by National Institute of Standards and Technology.

Congress has an opportunity now to improve and expand upon these programs. It was necessary to bolt on cybersecurity to existing programs in the past, but it is now time to ensure that these programs are impactful and remain sustainable. To remain sustainable, Congress should expand the current programs in connection with the cyber workforce to (1) expressly authorize and appropriate CISA to carry out the responsibilities of DHS where appropriate under existing law, (2) provide resources to increase the number of internships and apprenticeships available to qualifying students from high-schools, 2-year community colleges, or 4-year universities, and (3) provide incentives to Federal and non-Federal entities for jobs placement to soft targets like our water and energy systems.

3. *Policy Solutions to Better Integrate Technological Solutions for Mitigating Cyber Risks*

Eliminate “Tech-Debt.”—Technical debt, resulting from legacy IT and unsupported technologies, creates risk to operations, cybersecurity, and resilience, and creates inefficiencies and wasteful spending. The U.S. Government and critical infrastructure providers must focus on eliminating technical debt by identifying existing technical debt and then modernizing IT infrastructure, including moving to the cloud and deprecating legacy IT systems.

Build Cyber Resilience and Response Capabilities.—The choice between defense and offense is not binary. A game-winning interception steals the advantage from the offense and puts the team on the scoreboard. That’s an offensive defense, and a principle our cyber resilience must consider. Continued investments in automated recovery, real-time threat detection, and security operations center (SOC) modernization will further advance the ball here.

Strengthen Critical Infrastructure as part of our National Defense.—We need to correct foundational weaknesses in our Nation’s critical infrastructure and defense systems, focusing on (1) securing supply chains, (2) protecting sensitive data, and (3) ensuring resilience against unauthorized access and emerging vulnerabilities. A legislative agenda focused on implementing secure-by-design principles, upgrading supply chain standards, and fortifying critical digital and physical systems will fortify our critical infrastructure against nation-state threats.

Promote the Use of Artificial Intelligence (AI) to Transform Cyber Defense.—We have already seen the benefit of AI to cyber defenders, including using AI to more quickly identify threats and new vulnerabilities, and scale cyber talent. The Federal Government should build on this success to accelerate the development and deployment of AI and explore ways to improve the cybersecurity of critical infrastructure and small and medium businesses using AI. The Federal Government can achieve this acceleration through (i) funding of public-private pilots on the use of AI to enhance cybersecurity in critical infrastructure sectors, (ii) funding for large-scale, labeled datasets to make progress on cyber defense research, and (iii) prioritizing research and development on human-AI interaction methods to assist with cyber analysis and incident response.

Advance Threat Detection and Intelligence.—The need for advanced threat detection and intelligence capabilities to counter both known and emerging threats is certain. A combined Congressional and administrative agenda could focus on integrating AI, advanced analytics, and threat intelligence to enhance situational awareness and preempt adversarial actions in cyber space and the information domain. Constant vigilance—like a digital See Something, Say Something program—will enable the foresight needed to defend and defeat malicious cyber actors. Further, to enable identification of threat activity, CISA’s capability to hunt for and identify threats across Federal Civilian Executive branch agencies under 44 U.S.C. 3553(b)(7) must be strengthened. This includes developing the technical capability to gain timely access to required data from Federal Civilian Executive branch

(FCEB) agency endpoint detection and response (EDR) solutions and from FCEB agency security operation centers.

Enhance Identity and Access Security.—Distinguishing between our digital presences is—knowing who's who, and that you are you—is of paramount importance for cybersecurity. Compromises of identity and authentication are a leading attack vector that our adversaries exploit year after year; weak identity infrastructure also provides adversaries with the quickest and easiest way to monetize stolen data, given that many of the identity solutions we use on-line are built around the premise that “knowing several things about you” means “someone is you.” Solving this will require that America addresses the gap between the paper and plastic credentials—such as driver's licenses, birth certificates, and passports—that work in the physical world and the lack of any digital counterpart that can be used to prove who you are in the on-line world. This is an area where Government must play a bigger role—in that Government is the only authoritative issuer of identity. Likewise, knowledge-based systems for identity proofing are vulnerable, so too are our knowledge-based systems such as passwords for authenticating. We need to continue to drive the adoption of more modern, robust authentication solutions such as FIDO passkeys and security keys that can stop phishing attacks cold. Identity and access management (IAM) remains a pillar of zero-trust architectures—and encouraging both Government and private-sector organizations to accelerate their adoption of a unified identity security program can streamline efforts to prevent unauthorized access, phishing, and email-based attacks.

C. CONCLUSION

The global cyber threat landscape requires a coordinated, proactive approach combining legislative action, technological innovation, and operational collaboration. By addressing these challenges through the framework I've outlined, we can better protect our national security interests while fostering innovation and economic growth.

Chairman GREEN. Thank you, Ms. Walden.

Members will be recognized in order of seniority for their 5 minutes of questioning. I'll remind everyone to please keep their questioning to 5 minutes. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning.

Over the last year, the U.S. Government has discovered a number of PRC state-sponsored threat actors deeply embedded in and across the Nation's critical networks. Volt Typhoon, Salt Typhoon, Flax Typhoon, and most recently Silk Typhoon have compromised our critical infrastructure, hacked sensitive communications, breached Federal work stations, et cetera.

I appreciate Mr. Wales' comment about these names seemingly masking the real true identity of the threat, and I take that—I take that to heart. We need to call China out aggressively on this. It's alarming that most of our critical infrastructure systems have been violated right under our noses.

Mr. Meyers, can you explain the PRC's playbook on how each of the typhoon operations or how China's cyber war against the United States, how they're doing it?

Mr. MEYERS. Thank you, Chairman. China has engaged in, as I mentioned, a maturation in how they conduct these operations. Today, they're using exploits that target external-facing devices that are connected directly to the internet that effectively bridge enterprises to the internet.

These devices are often unmanaged. In many cases, they may be legacy or have proprietary capabilities. That means that they don't run modern security tools. China is also nationally—

Chairman GREEN. Can you give an example of one of those? Like is it—are we talking about a Fitbit on your wrist, or what are we talking about?

Mr. MEYERS. Sure. Like a router or a VPN concentrator, things that are meant to connect the enterprise to the network or allow remote users to authenticate in or some of the——

Chairman GREEN. Some of the nodes, so to speak, between silos?

Mr. MEYERS. Yes, sir.

Chairman GREEN. Got it.

Mr. MEYERS. These are highly-prioritized and highly-valuable targets for these threat actors. They have nationalized their vulnerability research program.

In 2018, for example, they changed the national security law in China, and all vulnerability research has to be submitted through that Chinese Government, whereas here in the United States, we follow something we call responsible disclosure. Where if I find a vulnerability in a product, I notify that product vendor in order to try to get it fixed.

They're effectively nationalizing that resource so that they can use that for exploits against American technology and American companies.

Once they gain that access, they attempt to remain stealthy, and either conduct espionage in order to inform political and military decision making. Or in the case of VANGUARD PANDA, also known as Volt Typhoon, the propositioning that we've discussed here, which would be potentially useful to bring down some of these networks that Mr. Montgomery mentioned in time of conflict.

Chairman GREEN. One of the questions I have of all of you—and I'm not going to ask for an open answer today—but I would like to ask if in writing, you could give your opinions and thoughts on how we address the issue of first to market for software and the vulnerabilities that it creates, that incentive to be the first to market. I get the economic benefit, the competitive advantage that comes from being first in market.

What can we do as a Government to not suppress, you know, our economic competitiveness, but at the same time, address something that's very difficult, and that is the vulnerabilities that come when software companies rush stuff to market?

So again, not for an answer today, but if you would, I think that's something that really important and on my—to tackle this Congress list.

I want to ask, or just, I only have a minute. Rear Admiral Montgomery, you mentioned the National Guard and their importance in the defense of the Nation. One of my National Defense Authorization Act amendments last cycle—I am going to bring it forward again in this cycle—is to put a cyber defense unit, National Guard unit in every State. As much as to help, you know, our answer national defense, but really because the States can then, you know, put those guys on Title 32 and use them in the event that—because our local governments and our States are getting hammered just as much as the Federal Government is. I wanted to get your thoughts on that while I had a few seconds.

Mr. MONTGOMERY. Right, I agree, and I agree for several reasons. No. 1, Governors have authorities at the State level that the Federal Government doesn't have. So actually having them local like that is good. No. 2, they have relationships within the community already. They come from companies there. I do think you need

it wide-spread because the State will lend, you know, disaster response to a State 6 or 7 States away. Because they can look at a weather map and say, "I'm not going to have the same event." But if a cyber event starts to unleash itself, Governors are not going to be that comfortable lending their limited cyber capabilities to a State that doesn't have them.

So I do think there is value in having a more robust National Guard capacity, and having it across all 50 States and 4 territories is probably the right answer.

Chairman GREEN. Thank you. My time has expired. I now recognize the Ranking Member for his 5 minutes.

Mr. THOMPSON. Thank you very much, Mr. Chairman. I applaud your effort on identifying cybersecurity as a critical area for this committee to look at. If I would capsule the testimony, we do have a problem. The question is, are we addressing it in the best manner? One of the things we did was create CISA as part of the fix.

I guess the question is: Do you see a continued role for CISA? Is there some other roles that CISA might play since that's kind of where we are today?

I'll start with you, Mr. Meyers, and we'll kind-of go down.

Mr. MEYERS. Thank you, Ranking Member. We would happily work with any Federal agency that is charged with securing the cybersecurity of the United States. As far as which agency is appropriate, I'd defer to the Federal Government on that one.

Mr. MONTGOMERY. I do believe that we need a CISA, and the specific one that you all have authorized. You've worked the last 4 years to modify CISA's actual authorities year after year. I do think I'd like CISA to focus on their role as the risk manager for the country. In other words, bringing together risks from all the different sectors and understanding which are the No. 1 risk areas that we need to address. I had pointed out rail, ports, and aviation. That cuts across multiple Federal agencies. So you do need one quarterback of the team to bring together all the different risks that they've assessed, and provide that guidance.

The current—Brandon in his last job, CISA, made a recommendation to the White House for that. The National Security Memorandum-22 that came out gave them kind-of a lukewarm responsibility. I'd give them the full-on responsibility as a sector risk management leader for the Federal Government, and making sure we work well in a public-private collaboration.

So yes, we do need a CISA. We probably need a CISA that's envisioned differently than the last 2 Presidential administrations have aligned it.

Mr. WALES. So CISA is essential, both because it has unique sets of authorities and resources to tackle this problem. Only it has the authorities necessary to move the Federal Government in terms of protection of the .gov in terms of providing both capabilities to agencies and helping departments and agencies across the Government move to a more common baseline. I think we have seen with Congressional support in terms of authorities and resources, that since the SolarWinds attack in 2020, there has been a remarkable change in the degree of protection and security we have of our Federal networks.

I think as you look to the private sector, again, CISA's unique authorities in terms of engaging with industry to be able to have protected conversations serve as a focal point working with other sector risk management agencies. Those are unique authorities, capabilities, and expertise resident in CISA. So that needs to continue.

Now, how do we grow it? How do we refine it to make sure that we can tackle the scale and pace of a threat we faced is a challenge that we are all going to need to grapple with. But that—all of it continues to point to the urgent need to continue those capabilities.

Ms. WALDEN. I am going to echo my colleagues here. CISA is absolutely essential to the defense of our critical infrastructure. This committee has done some powerful things for CISA and I think needs to continue. One is what I mentioned, CISA 2015. The superpower for information sharing, that liability protection, that encourages the private sector to engage—could be improved, but that is a key superpower.

Another is that CISA is formed as a national coordinator for Federal, civilian, Executive branch agency defense of critical infrastructure. I think that needs to continue and, in fact, should be improved.

There is language in the Homeland Security Act that allows CISA to provide technical assistance upon request to anybody that needs it, prioritized by critical infrastructure. That is key. But also strengthening CISA's ability to do that across borders, recognizing that our digital infrastructure is global in nature. CISA needs maybe some clarity on how to do that, provide that technical assistance when requested internationally as well.

Mr. THOMPSON. Thank you very much. Mr. Chairman, I think it's clear that whatever CISA's end up being, that it appears that at least 3 of the 4—and maybe the fourth witness if it's CISA, I'll work with CISA. That we need to make sure that that mission that CISA presently undertakes is maintained and with some of the enhancements offered, the coordination, and other things, I think, is very important. So with that I yield back.

Chairman GREEN. I thank the gentleman. I now recognize the former Chairman of the committee and committee—or the Chairman emeritus, Mr. McCaul, from Texas for 5 minutes.

Mr. MCCAUL. Thank you, Mr. Chairman. Thanks for holding your first hearing on this very important topic, and as the Ranking Member stated, a very bipartisan issue. The Ranking Member and I passed the Cybersecurity and Infrastructure Security Agency Act in 2018 because it was a civilian agency we thought best capable to interact with the private sector.

Since that time, I believe it's stood up its capabilities, its credibility. But the world is on fire today. It's a far more dangerous place than it was in 2018 from a cybersecurity perspective, particularly, when I look at China, Russia, Iran, or North Korea.

I was sanctioned by China, I'm the target of a disinformation campaign by China, along with 3 other Members, one of whom now is a Secretary of State, Marco Rubio. So I've kind-of first-hand witnessed this.

But I think one of the most frightening things to think about is this ability to preposition malware on critical infrastructure to give

them the capability to turn the switch off at any given time, and then to bring darkness to the entire East Coast, or to ports, you know, in New Orleans or Houston.

Can you—maybe, Admiral, start with you—explain how that exactly works? What can we do to fortify and strengthen these critical infrastructures?

Mr. MEYERS. Thank you for the question.

Mr. MCCAUL. I'm sorry, Admiral.

Mr. MONTGOMERY. Thank you, sir. No, you're right on. That to me this was a prompt jump. In other words, what we discussed previously was intellectual property theft. There has been an espionage.

This operational preparation to the battlefield, it is a war-making action, and, you know, we have to take it much more seriously. I think that we—you know, the idea that they've prepositioned malware or that they have capabilities that lie in wait that can come out at the right time as we're making a decision to move—you know, to respond to a crisis in Taiwan or crisis in the Baltic States. TRANSCOM operates on those unclassified networks with civilian systems.

This is why I think former Representative Waltz is right in the sense that we have to go on the offensive. We now have to actually publicly execute operations against Chinese cyber infrastructure to say: We know you did this, we know you used this infrastructure to do this, and we are going to remove that infrastructure from your capability.

Look, we may sacrifice a tool, we may sacrifice an access, but I think the military—Cyber Command and intelligence communities have lots of tools and lots of accesses.

What we need to demonstrate publicly—and we should attribute it to ourselves—say we did this because of what you did. Otherwise, the Chinese are going to keep doing what they're doing.

Mr. MCCAUL. I totally agree. We need to call them out for this. We know that in the event of an invasion with Taiwan, they will shut down their entire grid and shut down all of their cyber—and including probably hit the West Coast of the United States at the same time.

Mr. MONTGOMERY. How crazy would we go if we found 20 satchels of explosives strapped to different electrical power grids or port cranes around our country, and could attribute it to China or Russia? We would seriously be moving forces and say this is completely unacceptable behavior. But somehow in cyber space they get a pass. That's not right. We need to be more offensive about this. The bar for taking action has got to be lowered down to one that makes America and our infrastructure secure. Right now it is too high.

Mr. MCCAUL. I think the physical analogy is always accurate, first, from the OPM hack occurred 23 million security clearances stolen. If you imagine Chinese actors are caught at OPM actually stealing that data in person, and we tend to think cyber somehow are not that—that it's different, and it's really not.

Mr. Wales, can you in my remaining time—this unholy alliance I call between China, Russia, Iran, and North Korea, do you see any, in this alliance, any formation of working together in the cyber threats base?

Mr. WALES. So I would say there are very—there are some but limited connections at this point in part because there is not a significant degree of trust amongst those countries, despite their willingness to work together in very isolated places. They have also been caught conducting operations against each other, which is one of the reasons why they don't have a type of alliances, like say the United States does, with its Five Eyes partners, where it is much closer, sharing of information, conducting joint operations, et cetera. We don't see that yet amongst our adversaries. But that is changing. We are seeing closer connections in places like Ukraine, in terms of Russia, Iran, North Korea, et cetera. So we obviously have to carefully watch that space very carefully.

Mr. MCCAUL. Has the Cyber Diplomacy Act helped coordinate and deal with that on a defensive side? But I know my time has expired. Thank you, Mr. Chairman.

Chairman GREEN. The gentleman yields. I now recognize the Ranking Member of the Cybersecurity and Infrastructure Subcommittee, Mr. Swalwell, the gentleman from Palo Alto, California—the Bay Area.

Mr. SWALWELL. Thank you, Chairman. This is an important topic. It's a bipartisan topic. Andrew Garbarino and I worked very closely together on the subcommittee. But as the senior Californian on the committee, and a committee that has jurisdiction over emergency management, I just briefly wanted to express my heartbreaks and beats for the people in the Los Angeles area where 28 have died, thousands of structures have been lost, brave firefighters and first responders continue to battle the fires today as unseasonable and unpredictable winds ravage the area.

My ask of my colleagues is to just work with the Representatives from that area as we have worked with Representatives from every area in America that's been affected by disaster before. We've seen in Tennessee, for example, since 2020, \$39 billion from disasters. Since 2020, Texas has had \$68 billion in disaster damage; Louisiana has had \$34 billion from Hurricane Francine; Mississippi has had \$30 billion; Florida hit by Hurricane Milton and many other hurricanes has had \$30 billion; New York has had \$31 billion in damages; Georgia has had \$49 billion in damages; Alabama has had \$32 billion in disaster damages; Oklahoma has had \$30 billion in disaster damages; Arizona has had \$9 billion in disaster damages; South Carolina has had \$31 billion in disaster damage; Colorado has had \$22 billion in disaster damage; Pennsylvania, \$41 billion; and North Carolina \$37 billion.

It's not a matter of if a disaster will hit your district or area, if you are in Congress, it's just a matter of when. The theme has always been that we come together. I hope that's the case now.

Last week when I visited one of the affected areas, I stood with a mother at what was once the site where she and her husband raised their 2 little kids. As she looked for any memento that she could take back to the kids, she saw that their lives and their home had been reduced to complete ash. She found a shiny metal piece in the ash and noticed that it was a little bowl that her daughter had played with in her make-believe kitchen. That was all she walked away with to take back to her kids.

She didn't point fingers. She didn't put on a Republican jersey or a Democratic jersey. She just expects that the people who represent her will stand with her and help her find relief in the worst time of her life and the lives of her neighbors. I think that's why we all do this job.

So, Mr. Chairman, I look forward to working with the committee to make sure that wherever disaster hits, we stand up for it.

I'm going to briefly now just pivot to Admiral Montgomery. I appreciate your service, sir, to the country. I have worked in a bipartisan way, and the Chairman has supported this work to try and reform CISA, particularly as it relates to JCDC, the Joint Cyber Defense Collaborative, and to set more structure and scaffolding around how individuals are admitted into JCDC, and how they could exit if they're not faithful partners to it.

Do you see any needed reforms at JCDC?

Mr. MONTGOMERY. Yes, sir, thank you, and I do. I appreciated the provision you put forward last Congress. I would only say, I would add to it. We need to move the JCDC beyond a slack channel, which is what it is right now. You know, a non-real-time information exchange. We need to get the real-time information exchange.

When the Congress actually passed the provision that the JCDC operates out of, it's called the Joint Cyber Planning Office. We had other—I was running the cyber space operation when we put that forward. We had other elements to that that were necessary. Those have not yet been passed. I think they need to be authorized, because I think the JCDC to be effective is to have a planning element, an information sharing element, which at the speed of data, so you can get threat information to private-sector companies at the speed of data, and then an intel working group together, that might be at a more Classified level. That information sharing that has to be at the un-Classified level.

So I think the improvements in the JCDC through a provision would be an excellent assignment for the 119th Congress.

Mr. SWALWELL. That's very helpful. I'll take that back to our team. Thank you, Admiral. I yield back.

Chairman GREEN. The gentleman yields. I now recognize the former Chair of Border Subcommittee, Mr. Clay Higgins, from the State of Louisiana.

Mr. HIGGINS. Thank you, Chairman. Gentlemen and ma'am, thank you for being here. Ms. Walden, in your testimony, your written testimony, you referenced a cybersecurity bill. You stated that the bill would help bring coherence to the multitude of Federal regulatory approaches. The bill would have empowered the National Cyber Director to convene all of the relevant parties, including independent regulators, to develop a set of cross-sector minimum requirements that would have reciprocity baked in. Whereby a business that operates in multiple sectors or that is in the supply chain of many regulated entities would only need to show them at the baseline once. You stated on very confident, this approach would both meaningfully improve our cybersecurity posture and reduce compliance costs. I hope Congress will continue last year's momentum and move swiftly to enact this legislation.

Thank you for that statement, Ms. Walden, because that was my bill introduced in the 118th Congress, the Streamlining Federal Cybersecurity Regulation. We are indeed reintroducing that legislation in the 119th Congress. Mr. Chairman and my colleagues on both of sides of the aisle on this committee, we should move forward with that legislation, because it allows the industry sector to appropriately position themselves to spend less time and money in compliance with regulatory oversight, and more of the energy and focus on actually accomplishing their missions as it regards cybersecurity.

Ms. Walden, could you briefly discuss more in-depth how compliance with current cybersecurity regulations frameworks slows down the efforts to actually counter threats?

Ms. WALDEN. Thank you for that question, and thank you for reintroducing that bill. It is quite an important measure, I believe, for the overall building of resilience in our cybersecurity infrastructure, our digital infrastructure.

Right now across the 16 critical infrastructures, and I would add a few others that haven't been designated, some industries are highly regulated and also have wonderful controls that could do better. But I'm thinking like finance, for example. Other industries are just under the mark, and those are the ones that are most vulnerable.

So we need to figure out a regulatory approach to bringing the minimum baseline up so that we're all solving the same problem and doing it in an efficient and effective way. So——

Mr. HIGGINS. Yes, ma'am.

Ms. WALDEN [continuing]. The proposition that your bill brings forward is not only do Federal departments and agencies that have regulatory authority need to bottom-line, but the independent agencies need to do so. They need to find areas where there's duplicity. So we can eliminate that, find areas for reciprocity, and then cause all of our infrastructure to have minimum security requirements so that we're not causing them to just spend money on——

Mr. HIGGINS. Yes, ma'am, I agree. Then the Federal Government should be a partner with the cybersecurity industry, and the emerging technologies, including AI. We should aggressively support the industry and their ability to actually perform the mission. So regulations and regulatory oversight should not get in the way of that mission.

Mr. Meyers, my own confidential cybersecurity consultants that have helped me through 8 years in Congressional service to we the people happen to be partners with CrowdStrike. They have shared with me their assessment. They have the best technology, in their opinion, out there. Your over-watch team is outstanding.

So I would like to address to you, you've been in the business of tracking criminal and state-sponsored and national cyber adversary groups across the globe, and you deploy technologies to detect suspicious and malicious cyber behavior, and stop increasingly sophisticated adversaries—your words.

I would also ask you to comment on the lack of ability for the security sector to strike back. Would you just address that topic? I yield to the gentleman's answer.

Mr. MEYERS. Thank you, sir. The security industry, I think, is primarily meant for defensive posture. One that we take very seriously. I appreciate your support there. I think that there is a lot to be done to partner with law enforcement and those that have the intelligence community as well, and the military that have the title or authority to take those actions and to support those operations.

I am happy to share with you some of the previous successes in working through that. As I mentioned in the testimony, I think it's time that we increased the cadence of those operations.

Mr. HIGGINS. Thank you, and my time has expired. But just yes or no. If you had the legal authority to strike back, if Congress gave the cybersecurity industry the legal authority to strike back, would you be able to effectively identify a bad actor and do so?

Mr. MEYERS. We have the visibility to identify them.

Mr. HIGGINS. Thank you, sir. Thank you, Mr. Chairman, for the indulgence.

Chairman GREEN. The gentleman yields. I now recognize Mr. Magaziner, who also is a Ranking Member, and we appreciate his service, for 5 minutes of questioning.

Mr. MAGAZINER. Well, thank you, Chairman, and to the Ranking Member as well and my colleagues. It is great to be back and to be starting out with such an important and bipartisan topic.

Because the United States faces an incredibly dangerous and growing threat landscape with regard to cybersecurity. We face attacks from international cyber criminal groups, such as the Brain Cipher group, which attacked my home State of Rhode Island last month, stealing sensitive information from hundreds of thousands of Rhode Islanders. We also face increasingly brazen attacks from adversarial nations, including China, Russia, Iran, and North Korea.

We are all very familiar with the capabilities and increasing aggressiveness of China's cyber warfare campaign, most notably, Salt Typhoon, which impacted the data of millions of Americans, and Volt Typhoon which targets our critical infrastructure. It is also important that we not lose sight of Russia's aggressiveness against our country as well.

This past October, the Justice Department seized 41 internet domains being used by Russian hackers known as the Calisto Group, attempting to infiltrate U.S. companies and Government agencies. By the way, small-town America is not immune from this threat either.

Last year, a separate Russian hacking group, the so-called Cyber Army of Russia Reborn succeeded in disabling a water system in the town of Muleshoe, Texas, and a wastewater system in Tipton, Indiana, among others.

So my first question—and I'll throw this out maybe to Admiral Montgomery, or to any of you who have this information. If you had to guess, how many people, how many bodies is China, for example, putting into their cyber warfare campaign across all of the various organizations they have?

Mr. MONTGOMERY. This would be a guess, and I think if you go into a closed hearing, you might get a more refined answer, but I would say China is around 60,000.

Mr. MAGAZINER. Sixty thousand—

Mr. MONTGOMERY. To give you some comparison, the United States' Cyber Mission Force, our office aside, is about 6,400.

Mr. MAGAZINER. So China has 10 times as many people targeting us with cyber warfare as we have trying to defend ourselves. I assume that Russia also, through their assorted organizations, thousands of individuals?

Mr. MONTGOMERY. First, I should say we have an intelligence community element number that we don't discuss. But it's not 54,000 to close the gap.

Mr. MAGAZINER. Yes.

Mr. MONTGOMERY. Russia has a different number. Russia is a—they have both military and intelligence services that do actions, and they have contractors through what's called the IRA, a contractor group. There's a mix of people in there who do both. The numbers are bigger.

Mr. MAGAZINER. There are other criminal organizations. There are countless organizations and individuals targeting us with hacks, with ransomware, et cetera.

During Governor Noem's confirmation hearing to be Homeland Security Secretary, she said that CISA needs to be, "much smaller to fulfill their mission."

Do any of you agree that CISA should be smaller given the number of threat actors that are targeting the United States every day in the cyber space? I will take that as a no.

I'll also note, by the way, that she was 1 of only 2 Governors who turned down Federal grants for her State to strengthen cybersecurity as well. So there is a pattern here that is concerning that I'm sure we will ask her about when she comes before this committee, assuming she is confirmed.

I also want to commend—well, a number of the recommendations that have been made I think are terrific and make great sense. I want to commend you again, Admiral, for targeting the issue of critical infrastructure. I'm the cosponsor of a bill with Congressman Crenshaw, called the Contingency Plans for Critical Infrastructure Act to mandate that we identify and have contingency plans for critical infrastructure in the event of a cyber attack.

Also the role of the National Guard. I want to give a shout-out to the 102d Cyber Operations Squadron at the Rhode Island National Guard who do a phenomenal job.

I actually agree with, I think, a sentiment that the Chairman raised and a number of you as well, which is that we need to call cyber attacks what they are. They are attacks, whether they're targeting our data or our critical infrastructure.

I would just suggest that when foreign actors put misinformation into our information sphere as well with the purpose of trying to influence elections or turn Americans against each other by racial lines or religious lines or political lines, that is an attack as well. We need to call that out for what it is.

Americans have a First Amendment right to say whatever we want on-line, whether it's true or divisive or not, and that is Constitution-protected right. But Iran, Russia, China, et cetera do not have that First Amendment right when they attempt to influence our domestic condition by turning Americans against each other,

undermining election integrity, undermining confidence. That is an attack, and we need to call that out as well.

So I am over time. I thank you, Chairman, and I yield back.

Chairman GREEN. The gentleman yields. I now recognize the Chairman of the Transportation Subcommittee, Mr. Gimenez, from Florida for 5 minutes of questioning.

Mr. GIMENEZ. Thank you, Mr. Chairman. Before I move on to cybersecurity, as the only career firefighter ever elected to Congress, I want to share, you know, my colleague, Mr. Swalwell's condolences to what's happened in Los Angeles. But I also would like to see if you would consider doing some kind of a fact-finding trip by this committee to Los Angeles to determine what the conditions were prior to the fire, what the response to that fire was, and also what strategies, what mitigation strategies that we need to take in order to make sure it never happens again. Because there are certain things there that, you know, that caused me a little bit of concern about that whole situation.

Mostly what it is really about is the fuel and the control of the fuel. Because fire needs three things: It needs an ignition source, it needs oxygen, and it needs fuel. The ignition source, we don't know how to determine that yet. But when you have hurricane-force winds, you certainly have enough oxygen, it certainly appears that they had a heck of a lot of fuel. They didn't do a very good of maintaining that.

Mr. MAGAZINER. Will the gentleman yield for questioning?

Mr. GIMENEZ. Yes, I will.

Mr. MAGAZINER. Since Mr. Swalwell isn't here, I would anticipate what he would ask is would you also be interested in a fact-finding trip or study to see if, for example, the State of Florida has taken adequate steps to reduce flooding in the event of a hurricane or to reduce the—

Mr. GIMENEZ. Oh, absolutely. I think we are fantastic at what we do in the State of Florida, and—

Mr. MAGAZINER. I just want to make sure we have the same sort of—so you have every State, not just—

Mr. GIMENEZ. After every hurricane, we learn, and we change our codes and everything. So, yes, I wouldn't have any problem in doing that. You want to visit my town, Miami-Dade County when I was the mayor?

Mr. MAGAZINER. Sure.

Mr. GIMENEZ. Come out. I would be happy to show you what we've done. OK.

Now back to artificial intelligence—to actually cybersecurity. Does artificial intelligence have applications in cybersecurity on defense mechanism? So Mr. Meyers or Mr. Wales, if you want to answer that question.

Mr. WALES. Yes, and I actually would say that right now we're at a unique moment where artificial intelligence is being integrated into cybersecurity applications far faster than we're seeing adversaries able to weaponize artificial intelligence to launch attacks. So most companies, SentinelOne and among others, are working hard to make sure that their technology benefits from the latest and most modern artificial intelligence applications.

Mr. GIMENEZ. So, Mr. Meyers, do you agree?

Mr. MEYERS. Yes, absolutely. We've been using machine learning and artificial intelligence for the last 14 years at CrowdStrike.

Mr. GIMENEZ. Fantastic. What do you all think about yesterday's announcement of a half a trillion-dollar investment in artificial intelligence, so the Star Gate Initiative I guess? Anyone can answer that if they want. Do you know about that?

Mr. WALES. I read in the news. What I would say is, it is important, particularly in competition vis-à-vis China that the United States be a real leader here. So anything that we are doing as a Nation to ensure that artificial intelligence innovation is happening inside the United States is going to be good for both our security and our economic well-being.

Mr. GIMENEZ. If we win that race, would that be able to supplant the manpower advantage that our adversaries may have in that regard in terms of cyber attacks and our ability to defend them?

Mr. MONTGOMERY. I do believe artificial intelligence and machine learning can make a big difference in the speed with which you find accesses and develop tools.

One thing I would give Congress is as we see that \$500 billion get invested, the one area—I'm not for regulatory environment here—but the one thing I would regulate, much like we do at our national labs, is I would demand a level of physical cybersecurity around that most important intellectual property, the model weights, and things like that. Again, I wouldn't heavily regulate the entrepreneurial spirit, but I would regulate the security so that we maintain, any breakthroughs belong to us, and belong to United States companies, and eventually to the United States military that aren't easily stolen by our adversaries.

Mr. GIMENEZ. I believe that the artificial intelligence technology is a national security technology, much as any weapon system that we have, maybe even more important than any weapon system that we have. We have to maintain our advantage and keep it in a very, very, very secure place. Hopefully the artificial intelligence will be able to guard itself. OK.

Finally, do we have any rebound capability? In other words, what I mean by rebound, somebody attacks you, and then the response, the rebound to that is even worse than the attack so that you know that if you punch me in the nose, I'll cut your head off. Do we have that capability?

Mr. MONTGOMERY. Sir, that's what I was talking about with deterrence. You know, we've talked a lot about deterrence by denial here. That deterrence by cost deposition is the punch-back. Then defensively, we do have to have a rapid recovery. One of the things America is good at is getting back up off the mat when we're hit. But in cyber space, I don't think we're properly organized for that yet. This is more than FEMA. This has got to be—we call it continuity the economy planning. We've got to get working on that. So a better offense and a better ability to recover once we're punched in the face. Those are going to be the two things we need to win.

Mr. GIMENEZ. I know my time is up, and just a simple yes or no. Will artificial intelligence help us in that? Yes or no?

Mr. MONTGOMERY. Yes.

Mr. GIMENEZ. Thank you. I yield back.

Chairman GREEN. The gentleman yields. I now recognize Mr. Goldman, the gentleman from New York, for his 5 minutes of questioning.

Mr. GOLDMAN. Thank you, Mr. Chairman. I agree, I'm encouraged by the bipartisan nature of this hearing on what is increasingly an important and dangerous threat to our homeland and our security.

In the past, though, it has not been as bipartisan. In fact, in September 2023, more than 100 House Republicans, including the Chairman, tried to slash CISA's budget by \$3 billion, which was 25 percent of the budget.

Now, this is because many Republicans did not like the fact that CISA—that CISA had, at the time, said that the 2020 election was not stolen, and, “there is no evidence that any voting system, deleted or lost votes, changed votes, or was in any way compromised.” That CISA director was Chris Krebs, who was then immediately fired by Donald Trump. Mr. Wales you took over.

Mr. Wales, do you agree with Mr. Krebs's statement that there is no evidence that any voting system, deleted or lost votes, changed votes, or was in any way compromised, and that the 2020 election was free and fair?

Mr. WALES. Yes.

Mr. GOLDMAN. So part of the problem here is that even though CISA's misinformation and disinformation activities represent less than one-tenth of 1 percent of its budget, Republicans have tried to cut 25 percent of the budget. Governor Noem has made it clear in her hearing that she would like to limit and reduce the size of and role of CISA, which seems odd in this time when all we are hearing from our witnesses here is the increasing danger of cyber attacks, and cyber infiltration exacerbated by artificial intelligence.

We know Russia used cyber warfare to interfere in our 2016 election. We know China has tried to do the same. But it is not a partisan issue. Because Iran tried to do the same thing by infiltrating Donald Trump's campaign.

It is bewildering to me that given the CrowdStrike disaster with the outage, which dramatically affected my district with the Microsoft hacking that gave access to—gave China access to senior government officials' information, that we would be reducing the budget to address our cybersecurity.

One thing I want to address—Mr. Wales, and I'll ask you first—is what would the impact of reducing CISA's budget, or reducing the size of CISA be both in terms of our broader cybersecurity and infrastructure security as the Rear Admiral has talked about, as well as election integrity and preventing foreign influence in our elections?

Mr. WALES. You know, a lot would depend upon how that cut was allocated. But broadly, it would dramatically limit the ability of the agency to conduct critical missions. So that would include its ability to provide technical support to critical infrastructure. State and local governments who request assistance with actual cyber incidents, or conducting pre-incident assessments of their vulnerabilities, they could be hardened. It would compromise its abilities to perform its functions across the Federal networks in terms of both monitoring and responding to incidents, deploying

technology to ensure that Federal networks are protected by best in breed technology platforms. But just across the board, it would lessen its ability to respond at a time of significant cyber threats as being described today.

Mr. GOLDMAN. In terms of the election integrity work that CISA does, is it accurate that that is primarily focused on foreign actors and foreign interference?

Mr. WALES. Almost all of CISA's work when it comes to elections is actually focused on cyber and physical security-related work, providing assistance to State and local governments who request vulnerability assessments, scanning for vulnerabilities, conducting training, doing physical security assessments, increasingly as State and local election officials are concerned about physical security threats they may face. That is almost the entirety of the election security work. So any cuts to the CISA budget would affect its ability to support those officials.

Mr. GOLDMAN. CISA is the only, sort-of the only department within any Executive branch agency that provides that cybersecurity service to State and local officials who administer our elections. Is that right?

Mr. WALES. Yes.

Mr. GOLDMAN. Thank you. Thank you, Chairman. I yield back.

Chairman GREEN. The gentleman yields. I now recognize the Chairman of our Counterterrorism Subcommittee, Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman. I appreciate this hearing. I'll get right into it. When you look back at Volt Typhoon, Storm Typhoon—or sorry, Salt Typhoon, I mean, you know, the list goes on and on. I'm obviously worried about critical infrastructure, not just in my own district that includes energy production, but every other aspect of our lives.

So I will start with you, Mr. Wales. In the last Congress I introduced the Seven Act, which was—and I hope that we can mark it up in this committee this year and send it to the floor, because it's a coordinating piece of legislation that asks our Federal agencies to do the hard work of coordinating.

So who is the lead Government agency when it comes to responding immediately to a cyber threat?

Mr. WALES. So different agencies are going to bring different authorities to the table. You're going to want all those authorities to deal with the challenges that we have. So CISA has certain authorities in being able to help an entity recover from an incident, making sure they understand what's happened. But you also want, at the same time, the FBI that has—can use its law enforcement authorities to figure out who the adversary is, and are things that can be done to disrupt their infrastructure, impose consequences? There's coordination with the intelligence community that's going to be tracking adversaries overseas. So there's not necessarily going to be one person, because no one agency has all the authorities, resources, and capabilities that we're going to need to tackle that problem. What you want are those agencies working closely together.

I would argue from my time in and having just left, the operational coordination amongst the agencies working on cybersecurity is better now than it has ever been.

Mr. PFLUGER. Ms. Walden, how would you grade the response to, let's just say, Salt Typhoon to the cyber attack? Because I'm going to pull this thread just a little bit that there's no single agency that's in charge. There's a lot of stakeholders. But how is our response to Salt Typhoon?

Ms. WALDEN. Well, sir, I was—I think the response to Salt Typhoon was adequate and appropriate. I was not in Government as part of the apparatus at the time that Salt Typhoon was discovered. But I do think it was adequate and appropriate.

Mr. PFLUGER. Admiral Montgomery, you see—let's go around. How is our response, what can be better, and do we need a lead agency to help coordinate?

Mr. MONTGOMERY. Hearing those answers, you know, as 35 years in the military, I kind-of learn you need 1 leader. One agency needs to be in charge. I have never seen a military organization work with 2 leaders in charge. So the right answer is CISA. I think we have to create that condition. Look, do I think other people contribute to it, the Sector Risk Management Agency that's responsible for industry? Sure. But in the end, there can be only 1. That leader, I think, needs to be CISA. I think the Biden administration missed a great opportunity to do that in National Security Memorandum-22. Even though CISA was telling them to do it and asking for that lead responsibility, they did not get it. I think we need to, as we redo national security memoranda and things, I think an upgrade to that, to put CISA in charge—this is bipartisan issue. You know, this committee created CISA. You need CISA to be that leader on the Hill.

Mr. PFLUGER. You know, in the aftermath of the *Loper Bright* decision, the Chevron Deference precedent, Mr. Chairman, I think this is a perfect opportunity for us to be specific in this committee, and to take what Admiral Montgomery is saying and designate a lead agency, and actually tell the agencies what we want them to do, not just give them the open, blank chalk board to write what they think is best, but for Congress to take an oversight role.

In your written testimony, Admiral Montgomery, you used the term, "lying in wait" when you're referring to the Volt Typhoon attack. Who is lying in wait now? What is the next attack that keeps you up at night?

Then, Mr. Meyers, I want you to comment on the same thing.

Mr. MONTGOMERY. I think all of the axis of authoritarians could lie in wait. That's China, Russia, India, North Korea. But I think realistically, the countries that are thinking about that they need to stop an American ability to mobilize forces, or really weaken our economic productivity is China and Russia. I think China is the predominant actor right now. I think Russia is distracted by other things. I have no doubt that there is Russian malware in our systems with an ability to be accessed at a later date.

So it's China, Russia—and we got to keep our eye on—if I had to choose 1, I'd choose China.

Mr. PFLUGER. Thank you. Mr. Meyers, I'll give you the last 30 seconds.

Mr. MEYERS. Thank you, sir. These incidents are not over. Salt Typhoon is an on-going activity by an adversary as is Volt Typhoon or what we call VANGUARD PANDA. So this is something that we

need to continuously engage, we need to continuously identify, root them out, and put a stop to them and cut off their access.

So I would say that—I just want to make that point that this is something that’s on-going. We need to remain focused on it.

Mr. PFLUGER. Thank you for your testimony. Mr. Chairman, I yield back.

Chairman GREEN. The gentleman yields. I now recognize Mrs. Ramirez for her 5 minutes of testimony. Welcome back.

Mrs. RAMIREZ. Thank you, Chairman. Thank you, Ranking Member. Truly grateful to be back in my second term serving in this committee that I believe will need the leadership of all of us, and certainly those of us who have personal experiences with a lot of the work that we do here.

So I want to talk to you, Mr. Wales, a little here. You served as CISA’s executive director from 2020 until August of last year. In that capacity, you oversaw the execution of the agency’s operations. So you’re well aware of how CISA was investing its resources, correct?

Mr. WALES. Yes.

Mrs. RAMIREZ. So Governor Noem, Trump’s pick to lead DHS, has stated that CISA was far off mission from its work to combat mis- and disinformation, and that in courts, they were using their resources in ways that were never intended.

Mr. Wales, I want the record to be clear about how CISA spends its resources. To the best of your recollection, Mr. Wales, how much of CISA’s budget is spent on mis- and disinformation work?

Mr. WALES. The last time I looked at this, it was something less than \$2 million.

Mrs. RAMIREZ. So what would that be percent over the entire budget?

Mr. WALES. Far less than 1 percent to the \$3 billion budget.

Mrs. RAMIREZ. So less than 1 percent of the total budget. Has CISA mis- or disinformation work ever interfered with its ability to execute cybersecurity mission?

Mr. WALES. I don’t believe so.

Mrs. RAMIREZ. Thank you. As part of a bipartisan infrastructure law passed in 2021, Congress provided \$1 billion in new grants to State and local governments to enhance their cybersecurity. State and local governments have struggled, we know, to adequately defend our networks, exposing them frequently to cyber attacks, and putting critical public infrastructure at risk.

As funding for this program flows to State and local governments, we’re also seeing the important progresses it’s having and addressing in long-standing and doing investment in State and local cyber defense. Unfortunately, this program expires in September. At the same time, we continue to see a rise in global cyber threats.

So this is a question I have to all witnesses in the time that I have left: Do you agree, yes or no, that the State and local cybersecurity grant program should be reauthorized? Sir? Yes? Is that—I can’t see the names here.

Mr. MONTGOMERY. Yes.

Mrs. RAMIREZ. OK.

Ms. WALDEN. Yes.

Mrs. RAMIREZ. Thank you. Let me ask you a follow-up question, and this one would get a sentence or two from each of you. We are going to be fair here, so we want to make sure everyone gets a little time.

What are the national security implications if we fail to adequately defend State and local government networks? I'll start with you.

Mr. MEYERS. Thank you. Threat actors target State and local governments very frequently, and they understand that those are accesses that can lead to strategic or tactical objectives that will secure their goals. So, I think that we need to make sure that we ensure that those State and local entities, and to include school districts, are well-protected from the cyber perspective.

Mrs. RAMIREZ. Thank you. Mr. Montgomery.

Mr. MONTGOMERY. Sure. The State and local governments are the low-hanging fruit. They usually don't have 2 wooden nickels to rub together to increase their, you know, to spend on their utilities. Because we as voters don't like to let them increase their rates. But I will tell you the No. 1 thing they need to is work force. The best way to get it, that's the PIVOTT Act. So if you bring that back, this cycle, I think you're going to attack the No. 1 issue State and local governments have.

Mrs. RAMIREZ. Mr. Wales.

Mr. WALES. I would just say that State and local government agencies are the closest to the American citizens. So disruptions at the State and local level are ones that people feel quickly in their schools and their utilities that are provided in the public services that they often get. So, absolutely, this is an area where adversaries target, particularly ransomware groups, as well as nation-states. So it is an area that needs attention.

Mrs. RAMIREZ. Thank you, Mr. Wales. Ms. Walden.

Ms. WALDEN. I agree with all of my colleagues. I want to point out in everything that they've said is that State and local entities really need to work on their technical debt, figuring out how to resolve some of their legacy technologies so that they are able to withstand cyber attacks that are happening in their backyards every day.

Mrs. RAMIREZ. Thank you, Ms. Walden. It's clear that reauthorizing is going to be critical for this moment. Thank you so much. With that, Chairman, I yield back.

Chairman GREEN. The gentlelady yields. I now recognize our Chairman of the Cybersecurity Subcommittee, Mr. Garbarino, the gentleman from New York, for 5 minutes.

Mr. GARBARINO. Thank you, Chairman. Thank you very much for this hearing. I love how you had them place the PIVOTT Act in his last answer and say how we had to pass it again. That was well-placed there.

Thank you to all of the witnesses for all being here. It's great to see you all again. This hearing is very important, and I think your focus on China has been, you know, just—it's obvious that they are the No. 1 adversary. If we can combat and defend against China, we can probably defend against everybody else. Because they are the best at what they do. We have to be better.

I want to talk about what CISA should be doing. Are they doing what they should be doing? What else? What other authorities should we give them?

Mr. WALES, you were there for a very long time. You were executive director and acting director. What should CISA be doing that it's not doing? Should we give them many more authorities that they don't currently have to step up their game and defend against China?

Mr. WALES. Yes, so I would say that, you know, looking at CISA's 2 primary missions in cyber. No. 1 is to help protect the Federal Government's networks, and No. 2, to help support the security and resilience of our critical infrastructure networks.

In the Federal Government space, thanks to a lot of resources and authorities from the Government, I think CISA needs to continue the momentum.

We're in a much different place than we were in 2020 during SolarWinds. The Federal Government is far more secure today. It's the reason why Federal Government agencies identified compromises in places like Microsoft, because of the investments that Congress has made in both CISA and across the Federal Government. I think there it's about building momentum and keeping that going.

When it comes to critical infrastructure, it's a much more challenging problem. It's a much more crowded space. CISA's real role is to be that focal point and coordinate amongst all of the other agencies that are working in this space.

I do think CISA has sufficient authorities, but it's really an issue of scale. Can we meet the scale of the challenge with both technical assistance training? Do we have the right tools to bring to bear, to meet this challenge? I do think there are areas that need work. I'm hoping that the Trump administration will focus on how do we improve the operational collaboration, build on the framework that exists today with the Joint Cyber Defense Collaborative, but take it to the next level, continue to drive improvements in our ability to work side-by-side with industry on day-to-day operational cyber threats. I think that is where the most urgent need is.

Mr. GARBARINO. You talk about defending against the Federal networks. An Executive Order that was signed, I think, last week tried to do that with threat hunting. A lot of agencies don't like CISA participating on their networks.

Does the Executive Order go far enough? Is it something we have to act legislatively to tell—and everybody can jump in here—to tell these agencies, Hey, you have to let CISA do its job and threat hunt here.

Mr. WALES. This builds on authorities that Congress gave to CISA in the Fiscal Year 2021 National Defense Authorization Act that gave them the ability to threat hunt on Federal agencies without permission. That was important.

Then supplemental funding allowed a deployment of endpoint detection to response technology that gave the security sensors the ability to actually hunt on.

This Executive Order requires agencies to actually provide that sensor information to CISA that allows them to conduct that threat hunting. It is absolutely essential. That is the way that you spot

adversary campaigns early. It is the way you look consistently across agencies so you're not dependent upon the differences in capabilities at various agencies. The amount of staff, et cetera.

So I do think that part of the Executive Order is strong. I don't necessarily know that they need additional legislative authority. But it is something that is going to be important for the next administration to continue to push agencies to ensure that CISA has the level of visibility it needs to conducting the threat hunting that gives you the cybersecurity outcomes that you want.

Mr. GARBARINO. Ms. Walden, did you want to add something? It looked like you were getting ready to. If you don't, that's fine, I have other questions.

You talked over, Mr. Wales, about the information sharing, I think, is what you were getting at between private and public sector when it comes to critical infrastructure, because 80 percent or 85 percent of critical infrastructure is controlled by private sector. Do we have that type of information sharing now?

Mr. WALES. This is a—you know, I've been talking about information sharing since I joined the Department in 2005, starting in counterterrorism, not in cyber. There is always ways that we can improve information sharing. It has improved dramatically over the past 8 years, but there is a long way to go.

It's also a question of do you have the right private sector in the room, are you sharing information at a speed at which it can be effective in the cybersecurity context, and are people capable of using that information to improve their security in real time? I think there is a lot of work to do to make sure that that happens.

Mr. GARBARINO. Going both ways. I'm out of time. But I did just want to say before I end, Rear Admiral, your comments on continuation of the economy in your written statement is 100 percent, I think, on point.

We directed the Biden administration to come up with a plan, they failed, and I think this is a huge thing that we need to work on with the Trump administration. We have to come up with a real continuation of the economy plan, just like Congress bipartisanly directed the administration to do.

So with that, I yield back, Chairman.

Chairman GREEN. The gentleman yields.

I now recognize Ms. Pou for 5 minutes of questioning, and welcome to the committee.

Ms. POU. Thank you. Thank you, Chairman Green and Ranking Member Thompson, for holding today's hearing. I am proud to be among the newest Members of the Committee on Homeland Security.

My north Jersey district is just across the river from New York City. So many constituents remember well the horrific, unprecedented terrorist attack that occurred there 2 decades ago.

I take my appointment to this committee very seriously, and I am excited to work with my colleagues on both sides of the aisle and collaborate with stakeholders and experts to advance solutions to improve the safety and security of New Jersey and our Nation.

The Cybersecurity Information Sharing Act of 2015 is set to expire this year. Since its enactment 10 years ago, this law has created critical information-sharing partnerships and collaboration be-

tween the Government and the private sector. These relationships have enabled America to better respond to rapidly-evolving cyber threats, making the country safer.

To each of our 4 witnesses, can you please describe the benefit of the Cyber Information Sharing Act, but please detail, if you would, how would a lapse in this authority affect our Nation's security. Mr. Meyers or—

Ms. WALDEN. I can start.

Ms. POU. Ms. Walden. OK.

Ms. WALDEN. I can start.

Ms. POU. Thank you.

Ms. WALDEN. So the importance of the Cybersecurity Information Security Act, unfortunately, the same name—acronym, the CISA 2015—

Ms. POU. Yes.

Ms. WALDEN [continuing]. Is paramount. Because what it does is it gives liability protections to industry to share with DHS and through CISA, to share amongst each other in order to be able to at least, at a minimum, get rid of the low-hanging fruit. They are allowed to share cyber threat indicators and defensive measures for a cybersecurity purpose. They are protected from FOIA, they are protected from antitrust litigation, they're protected from sunshine laws, and et cetera and et cetera.

This is key—this is a key underpinning law that enables the JCDC, for example, that enables other vulnerability assessments that take place, that enables us to be able—the Government to be able to interface with industry at the speed of data.

Ms. POU. Thank you.

Mr. WALES. I would just add that, most importantly, it provides assurance to the industry that they will be protected. Some people may be willing to share without this law, but the reality is many won't because they don't have a 100 percent certainty that they're not going to suffer any consequences, whether through some type of litigation or suit.

So ensuring that it is reauthorized is critical for enabling cyber information sharing to happen between the private sector and the Federal Government as a whole.

Ms. POU. Thank you.

Mr. MONTGOMERY. I'd also remind that back 9 years ago, it was weakened significantly in the Senate before it was passed.

I think you should take a look at strengthening the liability protections for the companies in that legislation. At the same time, I would take advantage of the opportunity to integrate CISA, the Cybersecurity Infrastructure Security Agency, and to strengthen its ability.

As I said earlier, we have to get off of Slack channel. We have to have authorized a system for actual speed of data transmission. We've got to push the intelligence communities to figure out how to get that down to the unclassified level so that there's a benefit and burden to this to the private sector. They both benefit from much better intelligence from the Government and the burden is they've got to report—you know, they've got to report what they're seeing and work closely with the Government to pass on their information.

Ms. POU. Thank you. Very quickly, Mr. Meyers.

Mr. MEYERS. Thank you. Information sharing is critical for our success. It's us. It's the vendors, it's our customers, it is our partners in the Government versus the adversaries. It's versus China, Iran, North Korea, and so information sharing is really the essential building block of how we secure our infrastructure.

Ms. POU. Thank you. Thank you so very much.

I yield back.

Chairman GREEN. The gentlelady yields.

I now recognize the gentlelady from Georgia, Ms. Greene, for 5 minutes of questioning.

Ms. GREENE. Thank you, Mr. Chairman.

Before I get into some questions, I'd just like to point out that Mr. Wales, in your testimony you talked about Iran's cyber hacking attempts against the—President Trump's campaign this past election cycle and it undermining President Trump's candidacy and showing discord within the United States electoral process. So thank you for pointing that out.

While cyber threats from our foreign adversaries must absolutely be protected against, we also can't forget that our own independent cybersecurity agency, CISA, was more focused on conducting its own large-scale election interference campaign through its censorship-launders complex against our own people rather than bolstering our cybersecurity efforts and working to protect our critical infrastructure.

Just some brief stats. The average cost of a data breach in the United States amounts to \$9.36 million, almost double that of the global average. As you, Mr. Montgomery, testified, the FBI received reports of \$12.5 billion in cyber crime losses in the United States in 2023, an increase of nearly 20 percent over 2022, which is definitely alarming.

Ransomware attacks rose 74 percent from 2022 to 2023. Cyber attacks on critical infrastructure globally increased 30 percent in 2023.

One in 3 Americans—and this is shocking—were affected by health care data breaches last year. Government agencies were the third-most targeted sector from ransomware attacks in 2023. There are roughly 500,000 vacant cybersecurity jobs in the United States.

Mr. Chairman, that is a serious issue.

Most cyber attacks fall into a never-ending pattern; a threat actor often sponsored by a nation-state exploits vulnerabilities in the system. They exfiltrate sensitive data or encrypt it for ransom. Then there is an investigation into how it happened, who was involved, and what measures should be taken to prevent it from happening again. Then it happens again, and the cycle repeats, and we're all in a very serious dilemma.

Mr. Montgomery, in your testimony you talk about some specific offensive and defensive solutions that we can take to address the needs of our cybersecurity shortfalls. Could you elaborate a little more on that, please?

Mr. MONTGOMERY. Sure. Thank you. You know, I would highlight in that first we absolutely have to invest in our Sector Risk Management Agencies to make sure they're doing their job. It's shocking sometimes when you look at—like, Department of Energy

spends, what I think is probably the right amount, somewhere between \$50- and \$100 million a year on being a Sector Risk Management Agency, helping energy companies protect themselves. Then you go to the Department of Agriculture, and they're spending \$500,000, or Department of Education, they're spending \$250,000.

Most of us understand that's 2 full-time equivalents or 1 full-time—it's 1 human or 2 humans. That's just website management. You're not helping the 8,000 farms and food distribution networks out there with 1 person manning a website. You're not helping our 9,000 districts out there with 1 person manning a website.

We need more consistent focus, leadership from the top-down, Cabinet members down, on cybersecurity as a responsibility they have as a Cabinet member. Then, when appropriate, the funding to do—to do that kind of thing. So to me, that's the No. 1.

I spoke earlier about military mobility. If I could only focus on 3 things, it would be rail, aviation, and ports because if we don't get that right, China, Russia, doesn't matter. If they initiate combat operations that we're going to be involved in, we won't get there fast enough.

Ms. GREENE. Thank you, Mr. Montgomery. I completely agree with you. Those are very critical infrastructure things that we have to protect.

With AI being the biggest emerging industry and the technology industry, I'd like to ask each of you, how can we protect Americans, protect our Government, protect ourselves from cyber attacks, and how do you see AI playing a role in that, maybe for the good or for the bad?

Mr. MEYERS. I'll start. Thank you.

Ms. GREENE. Mr. Meyers.

Mr. MEYERS. Artificial intelligence can be one of the solutions to a lot of the problems that you highlighted. When we think about the cyber work force, artificial intelligence can take more junior analysts and make them more senior analysts by automating and helping them deal with complex problems at scale and at speed. Also to say that artificial intelligence in the security domain can be used to identify and quickly remediate these attacks. So there is a huge opportunity there.

The one caution I'll say is that I think in the next 1 to 3 years, we'll be seeing more and more organizations and businesses employing their own artificial intelligence, and that will create a situation where there's what we would call AI workloads that need to be protected. So we need to be thinking about how can we proactively start talking about protecting those AI workloads today before they become a problem in the future.

Ms. GREENE. That makes sense. Thank you.

Mr. Chairman, can we allow our witnesses to each answer?

Chairman GREEN. Very quickly, a yes, no. But we need to move on. So if you've got a quick yes, no, you can do a quick yes, no.

Mr. MONTGOMERY. Yes.

Mr. WALES. Yes.

Ms. WALDEN. Yes.

Ms. GREENE. OK. Thank you so much. Thank you for coming to the committee today.

Thank you, Mr. Chairman. I yield back.

Chairman GREEN. The gentlelady yields.

I now recognize Mr. Turner from Texas. Also, welcome to the committee, sir, for your 5 minutes of questions.

Mr. TURNER. Thank you, Chairman Green and Ranking Member Thompson. It's good to be with everyone.

What I notice is that there are the same running themes from each and every one of you. Let me just say that as mayor of the city of Houston, we faced thousands of cyber threats every year. Cyber work force, critical. The grants to State and local governments, critical. The cities and States under constant attack, a coordinated approach, collaboration, always important. That's why I'm a strong supporter of CISA. In fact, when it came into existence, we went thumbs up.

Aviation, the port, utilities, our water systems are under constant threat. As a mayor, that is something that kept me up every night. When we saw what happened in Atlanta, when the ransomware gangs took over, municipal police, costing the city a great deal. We all tried to intensify our efforts with layers and layers, but we simply didn't have enough money to do enough.

So let me applaud each and every one of you because each one of you said—I think, Mr. Meyers, the threat has increased 200, 300 percent. I think, Rear Admiral, you indicated a persistent vulnerability that exists. Each one of you, the same themes over and over again.

Let me just go directly to the Office of National Cybersecurity Director. Ms. Walden, during your time at ONCD, both as a principal deputy, national cyber director, and as acting national cyber director, you were part of the development of this new office.

How has the creation of ONCD strengthened our national cybersecurity, and what additional steps should the new administration take for a coordinated approach to cybersecurity across the Federal Government?

Ms. WALDEN. Thank you. So the National Cyber Director's Office was created to provide strategic cybersecurity advice to the President. So that, just as Admiral Montgomery said, we have some accountability and some responsibility from the very top all the way down. That should be true in the Federal Government as well. There were a couple of things that we sought to achieve.

The first is to make sure that we have a more defensible, more resilient digital ecosystem, and that includes State and local entities. That means that we needed to do 2 things. No. 1, shift cybersecurity risk so that it is not solely the burden of cities and counties and educators, and shift that so that it's more the burden of the Federal Government, of large enterprises, of producers, et cetera.

Then with that residual risk, once we buy it down, to build in resilience, not just in the technology, but the technology is important, the backbone of internet—Salt Typhoon showed us it's important—but in the work force, in the people and the ability to be able to maintain all the new technology. Doctrinally, who is in charge of what, when, how.

So the work that we did there came with it—that strategic work came with it a full action plan, and that full action plan allowed each department and agency to take on responsibility for a par-

ticular provision of that strategy. That allowed State and local governments to plug in. That allowed companies to plug in and to move the needle forward. That was the strength of the National Cyber Director's Office.

I'll point out the national cyber director was able to, with the Office of Management and Budget, prioritize the Federal departments and agencies, how to ask for Federal funding in order to be able to pursue that mission. That kind of central activity within the White House was important in the last administration, and I see it going forward.

Mr. TURNER. Thank you. Mr. Montgomery, in your role with the Cyberspace Solarium Commission, you allocated from the creation of ONCD. What success have you seen from this new office, and how important is it that the new administration empower ONCD going forward?

Mr. MONTGOMERY. I think Kemba did a great job as acting national cyber director, and I think as did Chris Inglis and Harry Coker as national cyber directors.

So I think the most important things are the budget control. We all know resources are what drive things. So having—maintaining that budget control, what I wish they could do is expand it to make sure that the Sector Risk Management Agency functions are being paid for.

The second thing I think they're really good at is the work force, you know, protecting those. So, again, they'll be critical when we do get The PIVOTT Act passed.

The third thing I think the most important for is getting this harmonization of regulation. We've got to reduce the regulation on our industries. So I think if they're able to do all 3 of those things, the next administration's director will be successful.

Mr. TURNER. Thank you very much.

I yield back.

Chairman GREEN. The gentleman yields.

I now recognize Mr. Luttrell from Texas for his 5 minutes of questioning.

Mr. LUTTRELL. Thank you, Mr. Chairman.

I've got a small nursing home that's located in one of my little small towns in my district, and they had a cyber attack. We called in—we called in CISA. We started going through the—checking the boxes, and the FBI came in.

What ended up happening is when the FBI came on board and CISA were working in parallel with each other, it turned kind-of into a proverbial fistfight, who was in charge. As this thing kind-of inched along, the result was that the nursing home didn't get any results.

You mentioned earlier, if you follow the chain of command—and that has to be 1 leader, 1 person in charge. The net has been cast out very wide given just kind-of the proverbial threat when it comes to cyber risk, cyber threat, cyber attacks.

Can you give me some refinement on the best course of action on how to decrease that problem set?

Mr. MONTGOMERY. First, thanks for bringing that up. You highlight that rural health care right now in small—small health care facilities are probably the greatest risk we have in the utility area.

The reason I say that is that if they get a ransomware attack, most of them have about 5 or 6 weeks of float.

That is, if they don't end the ransomware attack and fully recover their systems, within 4 or 5, 6 weeks, they could be out of business, and then the community loses its health care.

So first thing I'd tell you is HHS, Health and Human Services, has to do a much better job supporting these guys left of boom. What I mean is we're pushing hard there; it's like a fractional CISO program. What that means is, I guarantee that hospital you're talking about or clinic could not afford a full-time CISO to prevent this ransomware and recover from it.

Mr. LUTTRELL. Correct.

Mr. MONTGOMERY. What we need to do is have a program where they can access a pot of CISOs who come in, who have done ransomware hundreds of times, help that hospital get back on its feet and recover; not just pay the ransomware. That's the easy part. It's restructuring the systems. But you need specific CISOs to do that. But you can only afford about 10 days of that CISO, not 365 days of his or her \$400,000 salary.

So to do this, we need a virtual fractional CISO program for rural health care. So that's the first thing I'd do. That stuff you plan left of boom. Once the right—and you're asking me about the cluster that was right of boom.

Mr. LUTTRELL. Yes, sir.

Mr. MONTGOMERY. That cluster right of boom, that starts with the White House. That starts with a national security memorandum that clearly states who is responsible and who is in charge.

Now, at a very localized one like that, you know, it can be done by—there will be some who have a better regional footprint. But a larger one, it's clear to me it's CISA. You have to have a rule set for it, just like you and I had rule sets operating in the Navy. Without that kind of, like, structured command, I think we're going to continue to have failures like you saw.

But I would say there's things we can do left of boom to prevent these from being the small-business-killing events that they are.

Mr. LUTTRELL. Yes. Because I have to say, that was networked. So not only—it touched them all and took them to a knee. So thank you for that.

Ms. Walden, I thought your opening statement was amazing and very point-driven, and I appreciate that. You were in a digital crimes unit—you oversaw a digital crimes unit.

Can you give me some background information on exactly that entailed? Where I'm going with this is we're talking about Russia, China, Iran, North Korea, but make no mistake about it, there's some proverbial bad actors in the continental United States as well and in my district. I represent a small portion of Harris County, and sex trafficking is—actually, in Houston, sex trafficking is the No. 1 city in the country.

Can you kind-of talk me through—because what I would like to do is—we're in 2025. There's just no way in hell we're going to go back to analog. I mean, the digital revolution is here. We're not going to get away from it. As great as it is, it's terrifying, in a sense.

Can you give me a course of action moving forward that this committee or this administration can jump on top of to decrease that problem set?

Ms. WALDEN. Sure. First I want to correct something for the record. You've given me a promotion. I was not in charge of the digital crimes unit, but I was——

Mr. LUTTRELL. You're welcome. Happy birthday.

Ms. WALDEN. I was responsible specifically for going after the ransomware threat——

Mr. LUTTRELL. OK. I'm sorry.

Ms. WALDEN [continuing]. Platform, which was an incredible mission set. If you can imagine the large enterprises, like Microsoft or like Google, like——

Mr. LUTTRELL. Yes, ma'am.

Ms. WALDEN [continuing]. Et cetera, see millions of signals a day, and they have within their data set a lot of information that allows us to see when there's a threat actor. CrowdStrike can do the same thing. We can go after them using legal means, which is what I was in charge for, but also technical means, cleaning up our own networks because cybersecurity risk was borne by the larger enterprises should be, and they need to buy them down for all of its customers.

So what I would suggest is that we employ policy solutions—this committee can employ policy solutions to shift that cybersecurity risk burden to those that are more capable of buying them down. That means Microsofts of the world should be coordinating with CISA and sharing information back and forth. Microsofts of the world should be able to identify when there are threat actors, to immediately deliver that information. I don't mean to just pick on them.

Mr. LUTTRELL. Yes, ma'am, I got it.

Ms. WALDEN. You know what I mean.

Mr. LUTTRELL. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman GREEN. Gentleman yields. I now recognize the new Ranking Member of, I think, Transportation, right?

Ms. McIVER, congratulations, and you're recognized for 5 minutes for your questions.

Ms. McIVER. Thank you, Mr. Chairman. Thank you, Ranking Member, and to our witnesses for joining us today.

Cybersecurity is no longer just a technical issue. It is a critical national security challenge that touches every part of our daily lives.

I represent New Jersey's Tenth Congressional District, and I first—and I see first-hand the importance of protecting our communities, whether it's safeguarding sensitive information for small businesses, securing local hospitals or ensuring that critical infrastructure, like power grids and transportation systems, remain resilient against cyber attacks.

With that being said, in my district which is home to critical infrastructures such as ports, transportation hubs, and energy facilities that are vital not only to our State but also to our entire Nation, can you elaborate on what Congress can do to better protect and work with local governments and private-sector stakeholders

in districts like mine to secure these critical assets from cyber threats? That's to anyone who would like to answer.

Ms. WALDEN. I can start. I would recommend that Congress continue to explore State and local grant-giving opportunities to be able to reduce some of the legacy technical debt that exists across critical infrastructure.

I would also encourage that you explore opportunities to expand internships, externships to qualifying students and SFS programs, for example, or CyberCorps, be able to deliver to State and locals the talent that they need in order to maintain systems, to vet systems and respond to incidents.

Ms. MCIVER. Thank you.

Mr. MONTGOMERY. Ma'am, could I add on to that 2 things. No. 1, we need bottom-up support. What I mean by that is there are places where the Federal agencies are just too small or too under-resourced to regulate. We've noticed this in water, the 55,000 watershed.

So we've been pushing for something called a water risk and resilience organization. Representative Crawford introduced it in the last legislation. What that does is allow trade associations to work with Federal agencies in order to establish the right level of standards.

If I could give one more, ma'am. It's clinics. We've seen this at a—for example, Google sponsors them. But in addition—what that does is allow local community colleges and vocational schools to run programs where their cybersecurity future professionals can work with the local governments and authority and utilities to improve cybersecurity.

Ms. MCIVER. Thank you.

Mr. MEYERS. If I may also, as we just heard about the clinic or the nursing facility in Texas, and similar to the small businesses and the critical parts of the transportation infrastructure that you just mentioned, there is 2 issues that I think we can address. One is that there is a lack of cyber work force, which we've also heard about earlier today. Some of this can be countered by relying on technology, like artificial intelligence. But we can also work to bring more interns and bring more STEM into the lower level of schools, down to the junior high school level even to start to train the next wave of work force.

Also, as mentioned in my recommendations, I think there is things we can do to incentivize these businesses to invest in the right cybersecurity by incentivizing them to use managed security services that can help protect them left of boom, as we've heard. There's a lot of work that can be done today that will have payoff in dividends.

Ms. MCIVER. Thank you. Thank you for that. It's interesting that you brought up the idea about the talent, you know, making sure that we have folks in the pipeline who are, you know, trained in this field, especially as NJIT, which is a large university in my district, they have wonderful programs and I'm sure would love to partner and collaborate any way to make sure that we're pumping out, you know, the future, future employees to be able to, you know, work in this field.

Thank you so much for answering those questions.

With that, Mr. Chairman and Ranking Member, I yield back.

Mr. STRONG [presiding]. Thank you. The gentlewoman yields.

I'd like to thank Chairman Green, Ranking Member Thompson, our witnesses for being here today. I'd like to recognize myself for 5 minutes.

As my colleagues have discussed, the threats of our Nation's security and how it has evolved over time, becoming more sophisticated and in many cases more dangerous. Most alarming is the ability of cyber adversaries to cause chaos without even stepping foot on American soil.

We have seen reports of adversarial nations, state hackers, such as China and North Korea, working together to conduct ransomware attacks against global infrastructure. I saw it firsthand as the chairman of the Madison County Commission in Huntsville, Alabama, creating total chaos. You think about a multi-million dollar option that we ended up rebuilding our system more cost-effective than paying ransomware.

Mr. Montgomery, are you concerned about the cooperation among cyber actors who use the same tactics?

Mr. MONTGOMERY. I am. I'm not as concerned about the axis of aggressors yet sharing tools with each other like we see with North Korea providing munitions or troops to Russia and Ukraine. I am, though, worried that the sophisticated nation-state tools are becoming increasingly available to non-state actors and criminal actors, both in the United States and overseas.

I mean, it's not lost on us that Russia's ransomware went down—Russia's ransomware attacks against the rest of the world went down for 3 months after the invasion of Ukraine because those same ransomware criminals were actually nation-state actors and started to attack Ukraine instead of attack U.S. companies. That's since returned with a vengeance.

But what it means is, is that the nation-state and the criminal actors share tools pretty effectively, and that makes it much tougher on our companies.

Mr. STRONG. Thank you. Although all cyber actors have their own objectives, there's one goal they share, and that's harming the United States of America.

Mr. Montgomery, do you foresee the emergence of a cyber axis of evil; why or why not?

Mr. MONTGOMERY. As I just mentioned, I do think you're seeing it with the criminal actors starting to get tools that the nation-state actors have. Do I think over time they'll share? Yes. If you had asked me as a military officer 10 years ago, would North Korea send troops to Ukraine, I'd have said no. Would North Korea give up 20 or 30 percent of its artillery to the Russians? No. The rules have changed.

The axis of authoritarians are clearly operating in a much more integrated and aggressive way. It's only natural that this will eventually devolve down to cyber tools and cyber techniques and the sharing of best—of worst practices in that case.

Mr. STRONG. Nation-state actors appear to be undeterred from targeting us in cyber space. Whether it's Iran hackers, our water systems or PRC state-sponsored threats, the critical infrastructure, it is time our national security adviser—you think about it, Mr.

Waltz says—and I quote—“Start going on offense and start imposing a higher cost and consequences.”

Given the severity and scope of these threats, is it clear that cybersecurity must be at the heart of our homeland security strategy?

Mr. MONTGOMERY. Yes. I mean, I think all 4 of us in our testimony said that cybersecurity is rapidly becoming the most significant threat to our homeland. Look, there's stiff competition there. Missile attacks, physical attacks, but cyber attacks are clear and present danger today to our industry, to our Government, and to our military.

Mr. STRONG. Thank you. Mr. Wales, how can the United States better harness its cyber toolkit to go on offense?

Mr. WALES. Sure. So United States has some amazing capabilities in this area. I think what we have seen is it works best when it's done in tandem with defensive operations where we see what the adversary is doing domestically. That information is fed into Cyber Command, and it allows them to target adversaries in a more precise way. It has worked best in places where Cyber Command is targeting, for example, ransomware operators.

Because of the number of those attacks, we can quickly provide—defensive operators can quickly provide them information on additional targets to go after, but we need to find ways to make sure that that integration is happening. So that what they're learning overseas is being fed to defensive operators, and what defensive operators are learning here is being fed into offensive operations.

Mr. STRONG. Thank you, all.

The gentleman from Tennessee is recognized for 5 minutes.

Mr. OGLES. Thank you, Mr. Chairman.

Admiral Montgomery, you note that Iran, and specifically the Iranian Revolutionary Guard Corps, is aggressive in its cyber attacks of Israeli networks. They're also among the primary threats to our networks here.

How robust is our cooperation with Israel to assist each other in protecting against this common enemy?

Mr. MONTGOMERY. Thanks for asking that because, you know, Congress did pass an act directing increased and improved cybersecurity cooperation between the United States and Israel about 4 years ago, and we've seen significant improvements.

I would say that there's tiers of cooperation. Probably the top tier is the United States and United Kingdom. Through Five Eyes we have an extensive level—we have a very integrated level of cooperation both in cyber and cryptographic intelligence sharing. But I'd put Israel very high on the list. I think we share threat information smoothly and fluidly. Tools that we see—that we detect we share with each other.

Again, probably not on the same level as the United States and the United Kingdom, but very close. We have a very—a common shared threat in Iran. Thankfully, the Iranians—the Israelis have done a lot to deter Iranian action over the last 6 months with their extensive strikes into Israel, both kinetic—into Iran, both kinetic and non-kinetic.

But, yes, our cooperation with them is at the highest level.

Mr. OGLES. I was going to say, I think, arguably, Israel is in some ways our eyes and ears on the ground and, arguably, the roughest neighborhood in the world.

So as you look at our relationship with the United Kingdom, what could or should we be doing with Israel to enhance, increase that partnership, understanding we have that common and shared enemy?

Mr. MONTGOMERY. I do think that there are—there's probably a level of classification that we can increase, you know—of sharing that we could increase ourselves to even higher. But I would say, I think we do a very good job.

Frankly, the Israelis do a great job providing information to us on what they see. This is an alliance in all but paper. We share information closely. We share a common threat. We provide reference to Israel in a very useful way.

So I think we're doing great work. The real order in there is continue what we're doing.

Mr. OGLES. Yes, sir.

Mr. WALES. I'll just add from a defensive perspective in the post-October 7 when I was in CISA, we were sharing every single day with the Israeli National Cyber Directorate information on what we were observing in terms of potential actors looking to target Israel. Those were from nation-states, non-nation-states who were in that environment looking to pile on.

That information sharing consistently was built on a decades-long relationship that we had established.

Mr. OGLES. Well, Mr. Wales, since you jumped in here, in light of the Silk Typhoon intrusion at the Treasury Department, how would you assess the adequacy of Treasury cybersecurity posture?

Mr. WALES. So, you know, I think the compromise of Treasury was interesting because, again, using—going after a third party, in this case going after a third-party security application beyond trust, I think it—Treasury's security has dramatically improved, just like much of the Federal Government over the past 8 years.

But what I would say is we're forcing adversaries to go after more complex targets, launch more complex operations, in this case, again, using a third-party supply chain attack, which is good but it also puts increased burden on us as a country to make sure that we're looking for those more complex attacks, that we're managing third-party risk, that we're understanding how they can use supply chains to target our most critical systems.

What we can and what we should expect from technology providers to ensure that their software and the technology that they provide to both Government and industry is as secure as possible.

Mr. OGLES. Well, in that context, when you look at the third-party providers—and, obviously, there's a vulnerability there—in respect to Treasury and other agencies, how do they compare in mitigating that risk as you're forced to integrate and provide technologies for the consumer and for governments, et cetera?

Mr. WALES. I would refer you to people who are in Government now who may have a better sense of where Treasury stacks up. But I will say that I was—when I was last in, I was impressed with their level of capability.

Mr. OGLES. Yes, sir.

With that, Mr. Chairman, I yield back.

Mr. CRANE [presiding]. I want to recognize Mr. Brecheen from Oklahoma.

Mr. BRECHEEN. Thank you, Mr. Chairman. I thank you to the witnesses.

I want to just lay out some numbers. I think it's intriguing. Cybersecurity hacks are costing us, according to some reports, \$320 billion a year. That's under U.S. citizens. That's about 1 percent of our GDP, our Gross Domestic Product.

It's been talked about Iran, China, Russia, North Korea, and at the individual level people have to worry about their bank accounts. You have statistics that say that 1 in 3 Americans have been affected by health care data breaches alone, just in 2024. So there's so much to gain not only from our national security being hindered, but it is—Mr. Wales, you said in your testimony, they are preparing for war, talking about China and their—their desire as it pertains to Taiwan.

I want to throw an interesting concept out. The Constitution actually talks about in Article 1, Section 8 something called letters of marque and reprisal. This is something that's not—I alone am talking about. This is something that goes back even to legislation that was filed a few years ago.

If you think about, when you all have been talking about we've got to go on the offensive. We all recognize we've got a massive debt. There's a limitation to how much we can spend. Throughout our Nation's history, letters of marque and reprisal were the opportunity for people that—knowing that private entities were being attacked, our Government would issue very limited in scope information for private entities to go out and be able to capture, to hack back—and it was applied to this scenario—versus waiting on Government to respond.

Sometimes if you're a security firm trying to defend a private company—as the saying goes in terms of companies right now, there's 2 types of companies in this world; those that have been hacked and those that will be hacked—there's a delay. Why would we not empower the free market to hack back under very specified regulated rules, Constitutional in every manner, letters of marque and reprisal, go on the offense and employ what we know are really intelligent people in the technology entity, and we make it hard for people to want to go after America?

If they know that if they hack Americans under these very specific details, having to identify where the hack came from, that CISA can be involved with, we immediately hit back. It is a great deterrent for aggression for foreign nations.

I've got about 2 minutes left. Who would like to speak to that?

Mr. MONTGOMERY. I'll start only because I'm from the Navy, and the last, like—the last ship seizure was, I think, by the Navy in World War II under that—under a similar theory.

What I'll say is I would prefer that we actually developed a cyber force that could do this where we were robust enough. I first have to acknowledge that the right long-term answer, just like it was with special forces after 9/11, was to grow our special forces, to be the force we needed.

In the short term, on occasion, you know, you may need to use contractors to get yourself—to bridge yourself to that point, but I think the long-term preference is that we have military actors.

Now, to get at our point, the military actors in the cyber force don't have to be wearing a uniform, and we don't have to recruit people that look like Chairman Crane looked like when he was—when he first joined with the Navy. They could be a little overweight, they can have an unusual drug usage recently.

Mr. BRECHEEN. I've got limited time.

Mr. MONTGOMERY. So I would say—I would go for that. In the absence of that, we need to look at the use of contractor—of contractor—I would not go to independent companies.

Mr. BRECHEEN. Let me—because this—people say, well, you would open up the Wild West. It's already the Wild West. Some of them say, well, you don't know what would happen if you did that.

Don't you think that's what the founding era, when they issued letters of marque and reprisal, had to worry about is somebody unintentionally that shouldn't be impacted? Of course they did. So for anybody that says there's a risk of this, you're right. But our founders knew in open waters there was the same amount of risk.

The problem is, I contend, we're in a place where we think Government is the solution to everything, and that's why we have a \$36 trillion gross national debt, and we've got a limitation on fiscal resources.

I love what you're saying. Some of you come from a Government background. But maybe we don't need to just be looking at the status quo. Our Founding Fathers knew there were risks with this, but they put it in our Constitution, and they were brilliant.

Anybody else want to talk about this?

Mr. MEYERS. Just agreeing with—with Mr. Montgomery here. I would caution that there is potential higher—potential collateral damage as a result of uncoordinated—

Mr. BRECHEEN. Is there anybody who is willing to think outside the box on this? Not from a Government background. Do you not think the Founding Fathers also thought this thing through and then—oh, it could be dangerous to empower privateers to do this, but they did it. Think about Dunkirk.

There's a time when Government can't solve all your problems, and they ask 800 boats to go and help out. Dunkirk would have been a collapse absent utilizing the free market.

Mr. MONTGOMERY. I think I'm far enough outside the box recommending for a seventh military service and cyber force. So I'm going to leave my—

Mr. BRECHEEN. I'm pushing pretty hard, but we've got to think outside the box to the limitation of Federal expenditure.

With that, Mr. Chairman, I yield.

Mr. CRANE. Thank you. I now recognize myself for 5 minutes.

Thank you guys for showing up today. It's unfortunate that we don't have the FBI and anybody from Homeland Security here to testify before the committee.

You guys have all discussed numerous attempts to—and even successfully infiltrate by our adversaries to hack into our critical infrastructure. We've been talking about our health care system

today, the power grid, water infrastructure, corporate infrastructure, Federal agencies, et cetera.

I know Director Wray of the FBI has even been up here in front of Congress testifying along these lines. I believe his quote was Chinese hackers are positioned on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities if and when China decides the time has come to strike.

One thing that my constituents often ask me is, why is nobody in the Federal Government ever held accountable for their failures? I want to point out that I believe it was you, Mr. Meyers, from CrowdStrike, you actually appeared before this very committee in the last Congress and actually took accountability for some of your company's failures. Is that correct, sir?

Mr. MEYERS. Yes, sir.

Mr. CRANE. Knowing—knowing that—and that's one of the things that the American people are so frustrated about with the Federal Government. Nobody ever gets accountable. Rarely does anybody take any ownership of their failures.

Mr. Meyers, do you think some of your counterparts from the Federal Government today should take some ownership of some of the failures that have led to many of our adversaries acquiring access to our critical infrastructure that we've been talking about today? Would you like to see—would you like to see that?

Mr. MEYERS. I would like to see us move to a position where we're able to stop these things before they happen.

Mr. CRANE. OK. So you don't want to see any accountability? Mr. Meyers, you don't want to see any Government officials maybe sitting on this panel today take some ownership?

Mr. MEYERS. My role here is to—

Mr. CRANE. Gotcha. Thank you.

To that point, I want to give some of the other members on this panel the opportunity to take some ownership of some of the failures that have allowed the Chinese and others to hack in to some of our critical infrastructure.

Does anybody want to take any ownership since you guys have been doing this for a very long time? I'll start with you, Mr. Wales.

Mr. WALES. I would say that when I was in Government, we were very clear about where we needed to make improvements, where there were failings, where we had not invested enough in the right areas, where we needed to make changes.

I would say if I look back at—because I was acting director at the time as the SolarWinds campaign had emerged, was discovered—we identified that the Federal Government for too long had overinvested in some areas of network security and underinvested in endpoint monitoring, came to Congress and said we need authority to do this, we need additional funding, here is how we fix these problems because we were not in the right place. Since then, we have made dramatic improvements in the overall level of security.

So I think where we needed to be honest about the lack of capability in certain areas that has allowed certain attacks to happen, we've been clear about that.

Mr. CRANE. Ms. Walden, how about you?

Ms. WALDEN. I was part of the apparatus that created the Office of National Cyber Director so that, in the famous words of Senator King, Congress would have one choke—one throat to choke when something went down. I think what Mr. Wales said was absolutely true.

We made movements to make sure that we are all singing off the same sheet of music, playing the same soccer game, whatever analogy you want. But I think the failure was a lack of coordination for some time——

Mr. CRANE. Do you take any ownership in that, Ms. Walden?

Ms. WALDEN. In the lack of coordination?

Mr. CRANE. Yes.

Ms. WALDEN. I will own that I worked to make sure that we had better coordination.

Mr. CRANE. So none. OK. Thank you.

Are you guys—Mr. Wales, are you familiar with this report, “The Weaponization of CISA, How a ‘Cybersecurity’ Agency Colluded with Big Tech and ‘Disinformation’ Partners to Censor Americans”? I believe this was the Judiciary Committee.

Mr. WALES. Yes.

Mr. CRANE. Mr. Wales, do you think it’s appropriate to silence Americans for pointing out anomalies, data and policy changes in, you know, our last election or any election? Do you think that’s appropriate for you guys to silence Americans?

Mr. WALES. I think Americans have free—free speech rights, and they can say what they want.

Mr. CRANE. OK. When you were in charge of CISA, did you ever oversee the censorship of any Americans for whatever views they might have held, whether you agreed with them or not?

Mr. WALES. No.

Mr. CRANE. No? OK. We’ve been talking today about some of the things that we can do to increase and bolster our cybersecurity efforts, and I agree. I do think that we need to go on the offensive.

I believe it was you, Mr. Montgomery, you talked about, you know, if we had foreign state actors placing satchel charges and explosives on our energy grid or anywhere else, you know, we would raise holy hell, and it would be an act of war.

My question to you guys, my final question is, why aren’t we doing it?

Mr. MONTGOMERY. So I think for too long we’ve seen cyber as a non-military tool, and we just—you know, we saw it as a nuisance and criminal act or tool. That has dampened our response.

As you pointed out, satchel charges, you and I would be leading the charge to go find out who did this and hold them accountable. I just think with cyber, we take on this tempered approach that it doesn’t kill people, even though we now know it does kill people. There are morbidity rates at hospitals that increase because of ransomware attacks. We know this.

It’s an attitudinal change. I think on a bipartisan basis 5 or 6 years ago, we didn’t see things this way. I hope on a bipartisan basis going forward, we can see that we need to go on the offensive and hold these—hold a country that does this kind of operational preparation in the battlefield against the United States accountable for their actions.

Mr. CRANE. I got one more follow-up question. Mr. Wales, if this—if you weren't censoring American citizens in CISA, why was it going on?

Mr. WALES. I don't believe it was.

Mr. CRANE. So you completely disagree with this report; is that what you're saying?

Mr. WALES. Yes.

Mr. CRANE. You're under oath today?

Mr. WALES. Yes.

Mr. CRANE. OK. Thank you. I yield back to—the real Chairman is now back.

Chairman GREEN. First, let me say thanks to the witnesses for being here.

Ranking Member, I think it's time to recognize you for a closing statement. I mean, is there something—

Mr. THOMPSON. Yes. I'd like to enter something into the record.

Chairman GREEN. Oh, yes. Absolutely.

Mr. THOMPSON. Mr. Chairman, I ask unanimous consent to enter into the record a report entitled *Cybersecurity Policy Recommendations for the New Administration* from the Aspen Institute.

Chairman GREEN. So ordered.

[The information follows:]

STATEMENT OF THE ASPEN INSTITUTE

JANUARY 2025

CYBERSECURITY POLICY RECOMMENDATIONS FOR THE NEW ADMINISTRATION

With an ambitious suite of goals for your administration under consideration, we want to offer our recommendations and assistance with one set in particular: the party platform's commitment to "use all tools of National Power to protect our Nation's Critical Infrastructure . . . and raise the Security Standards for our Critical Systems and Networks and defend them against bad actors."

The cyber risks facing America present short- and long-term challenges. Cyber crooks, rogue nation-states, and terrorists often see the first 100 days of a new administration as a prime opportunity to attack during a time of transition. Both U.S. Government data and America's companies are at risk. As past incidents demonstrate, there is potential for disruption to our way of life: from mass theft of Government employees' personal information, to lines at the pump, to infrastructure security risks like Chinese military hackers in our water supply. These threats present your administration and Congress with a key window in which to act.

At the Aspen Cybersecurity Program, we do not just "admire problems." Instead, we have built a robust and bipartisan coalition dedicated to addressing critical issues and finding solutions. We work with top talent of current and former Government officials as well as leaders of industry across multiple sectors: including tech, telecommunications, manufacturing, retail, and defense. During the first Trump administration, we were honored to work closely with Federal law enforcement, the U.S. intelligence community, and others to find solutions.

The Aspen Institute's US Cybersecurity Group stands ready to help your administration tackle its cybersecurity goals. Whether it's offering your new team a sounding board, supporting important work in Congress, or getting input from an array of industry leaders, we look forward to supporting the work ahead in this area.

We recommend a few first steps for your consideration and further discussion:

(1) *PERSONNEL IS POLICY: DEMONSTRATE CYBERSECURITY LEADERSHIP AND PREPARE FOR IMMEDIATE RESPONSE*

Streamline cybersecurity leadership; White House cyber components as well as Federal departments and agencies with critical cybersecurity responsibilities are not organized efficiently. Redundancies, delayed appointments and vacant political positions can make it hard to develop coordinated and unified strategies, policies, and response efforts. You and your advisors have an opportunity to prioritize, clarify, and align roles to promote efficiency, economies of scale, and maximum impact.

(2) PRIORITIZE CYBERSECURITY REGULATORY ALIGNMENT AND STREAMLINING

Streamline regulations; there are too many and they are inconsistent. In your first administration, you prioritized cutting burdensome regulations; in your second administration, we recommend doing the same in cybersecurity policy. Prior reports have identified dozens of overlapping regulations and approaches that can waste resources and a balance must be struck between centralization and customization in terms of standards and regulation. In the Trump administration, all new requirements must be rationalized around simple core principles that appropriately balance national security and business interests, including small businesses and local governments. In this post-Chevron era, working with Congressional leadership will be critical.

(3) PARTNER WITH THE PRIVATE SECTOR TO PROTECT CRITICAL INFRASTRUCTURE AND HOLD BAD ACTORS ACCOUNTABLE

The current state of U.S. infrastructure vulnerability is unacceptable. Power grids, transportation systems, water supplies, and communication networks are all in jeopardy. You can send a clear message: the United States will defend itself against cyber aggression with the same resolve as it defends against physical threats. Everything from defensive measures to offensive operations should be on the table. Crooks, spies, and terrorists should be hunted jointly with key private-sector actors. Efforts to “defend forward” must be continued in conjunction with providing resources and assistance to critical, often overlooked entities such as small businesses and rural communities. Further, we must leverage the United States’ unique combination of innovation and capital investment to support and incentivize in areas of the world aligned with U.S. interests.

(4) CONTINUE BUILDING MECHANISMS TO MEASURE PROGRESS

Government efficiency depends on good data and clear-eyed analysis. We can’t understand what works without data. We need a repository of data in this area to know what to keep and what to cut.

(5) RESET THE DISCUSSION WITH IMPROVED COMMUNICATIONS AROUND CYBERSECURITY ISSUES

The White House has the world’s greatest megaphone. Using the White House bully pulpit is essential so that the American people know the stakes in cybersecurity and what steps they can take to be part of solutions. For too long we have been discussing these commonly agreed-upon cyber strategies with limited progress. To move forward quickly, it is imperative to advance a new understanding of cybersecurity from a technology problem for technologists to solve; to an issue of national concern that requires an all-hands-on-deck approach. Cybersecurity must be seen as what it is: (1) A key enabler of economic growth and national security and (2) a critical tool in the effort to counter nation-state actors like China.

Our network is prepared to help move these priorities forward, including the launch of on-boarding sessions for new Government leaders. These sessions, led by industry leaders, will focus on understanding the current state of the critical pillars of cybersecurity, the authorities and constraints of each department and agency, and best practices for moving the above priorities forward.

We look forward to hearing from you and your team and continuing the work.

ACKNOWLEDGEMENTS

This document is authored by the Aspen Institute’s US Cybersecurity Group members who brought forward their ideas and recommendations for Aspen Cyber staff, experts, and our advisors resulting in the above. These recommendations would not be possible without their deep experience across the public and private sector gained over decades and that continue to critically challenge how we improve cybersecurity and cybersecurity policy.

The Aspen Institute’s U.S. Cybersecurity Group is the leading cross-sector, public-private forum for promoting a secure future for America’s institutions, infrastructure, and individuals—in cyber space and beyond.

Mr. THOMPSON. Let me, just as a final point, thank our witnesses. It’s been very good. We almost are on track, but we’re getting there. I want you all to work with us.

Again, I compliment the Chairman on looking at this as a priority for the committee. We’ll get there. I just think that we have to plow through it in order to get to the finish line, and we ask

your indulgence. If you have something that I think is of note for the committee to consider, I'd encourage you to share it with us.

I yield back, Mr. Chairman.

Chairman GREEN. Thank you, Ranking Member. Thank you for your comments on just the bipartisan nature of this. It is really one team on this one because this is—this is critically important.

I want to thank the witnesses. All of you have been fantastic, pretty much echoing each other's comments, which that's a good—a good slate of witnesses when that happens. I also want to thank the Members for their thoughtful comments on both sides.

I have stated my priorities on the cyber arena, and I want to—since this is our first hearing and because it's our first hearing on cyber, I want to restate those. I think our greatest issue, our greatest threat to the country is the work force shortage. When we have 500,000 empty jobs, when the FBI director comes in front of our committee and testifies that if he took every single cyber person he had, put them on the China desk, he'd still be outnumbered 50 to 1, that circumstance can't continue. That's why we'll be reintroducing The PIVOTT Act. I really appreciate many of you have mentioned it, if not by name, you've talked—all of you have talked about it, the need for that.

Then this harmonization of what's out there in the Government, I think we're spending a lot of time, especially our private industry—and we all know that much of our infrastructure is managed by our private businesses. I think the rear admiral mentioned that specifically in his testimony.

You know, we ask of our private businesses all these different things, and every agency publishes things, and oftentimes they contradict one another. There's this compliance checklist and this compliance checklist, and they wind up spending all this time on compliance when they really should be spending time on cybersecurity.

So finding a way for—to harmonize the Government regulations that are in this space, I think, will free up a lot of energy and money to do cybersecurity. I can give example after example, but we talked about the liability issue. I think, Ms. Walden, you brought that piece of it up.

On the one hand, we're granting one group liability, and then the SEC is telling people, yes, OK, it takes 7 days to repair a breach, but you have to tell your shareholders and make a public announcement in 4 days. Well, why would you announce in 4 days that you've got a breach when it takes 7 to fix it?

Just this—some of this stuff that's coming out of the bureaucracy and maybe even out of Congress, too, just has to be harmonized and synchronized. That's my second priority.

My third priority is we've got to rethink—and this is why I asked each of you this, and I'm reiterating my question for your written feedback on how we address the economic models in the production of our software and our technology. Because first to market is creating vulnerabilities that are costing the Government—right?—as a vendor and costing private industry billions of dollars a year.

We have to get to a place—I don't know if it's certification. I don't know—there are many multiple courses of action here. Liability could be one. I mean, I know the businesses don't want to hear that, right, Mr. Meyers? It's OK. It's my turn.

But I understand—I ran a health care company. I get being first to market. It's competitive advantage. But, man, if you throw that piece of software out there and you've rushed it to market and, man, it's got a hole in it, we could all be screwed. So we have to figure out how to reverse this economic model.

Another converse economic model is the fact that it takes \$3,000 and a laptop in Russia for a punk kid to get \$5 million out of a rural nursing home. You know, that economic—he has no risk. He's not going to be extradited to the United States. We have to fix that economic model and make it more expensive for him or her to hack us than a \$3,000 laptop and the security of a foreign country that isn't friendly to the United States. So the economic models have to be adjusted.

We will reenact the cyber subcommittees thing that I started last cycle where we get the various subcommittees of each of—we're siloed in Congress; the Government is siloed, we're siloed in this whole cyber thing. We've got cyber subcommittees in Financial Services, we've got cyber subcommittees in, you know, HASC. We got—try to get those together, we got them together last year about a quarterly basis. We'll try that again. We're going to start that process again and start thinking a whole-of-Government approach to cyber.

I might ask all of you at some point to come back and talk—and present what you did today to that cyber subs group because we really do need a whole-of-Government approach.

I agree on the unity-of-command issue that you mentioned, Admiral. That is critical. I spent 24 years in the military and studied the principles of war at West Point, so I get that. You're right. Clearly defining who is in charge, that's really us—right?—in Congress. Defining those authorities and—so we'll work on that, too.

One of the things that kind-of worries me a little bit is if you use chemical weapons against the United States, we have a written strategic response to that. If you use nuclear—I mean, we have a first use nuclear, right? So we don't have a cyber response strategy, if you hit the United States, this is what's going to happen to you. I hope the new administration will take that issue on and come out with a statement that says, if you do X, we will do Y and it's well-known and articulated throughout the world. Because you can have all the capability in the world, if you don't have willpower to use it, then it just doesn't matter.

There were some comments made about Secretary Noem's refusal to take some Federal dollars. I just want to mention that that is not a reflection of her commitment to cybersecurity. She just believes in federalism, and she spent millions of South Dakotan dollars to create this program of cybersecurity in her own State. Implying that she somehow is opposed to cybersecurity, cyber protection because she chose not to take Federal dollars, I think, is a mistake.

The Members of the committee can also ask additional questions to you. They have a few days to do so, and I ask that you guys respond in writing. Pursuant to committee rule VII(E), the hearing record will be held open for such for 10 days.

Thank you again, and without objection, this committee stands adjourned.

[Whereupon, at 1:13 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR ADAM MEYERS

Question 1. Which “Typhoon” concerns you the most and why?

Answer. Response was not received at the time of publication.

Question 2. Please describe the Salt Typhoon threat as you understand it. Were Salt Typhoon’s tactics sophisticated? Is their activity consistent with other PRC cyber threat actors you have observed?

Answer. Response was not received at the time of publication.

Question 3. Please describe how Russia uses “living off the land” techniques. What are Russia’s objectives when it uses this TTP? How does Russia’s use of “living off the land” compare to that of China?

Answer. Response was not received at the time of publication.

Question 4. In your testimony, you described the urgency of the threat posed by North Korean cyber actors. What are tactics we should anticipate? Do you feel that the public and private sectors are equipped to address the threat posed by North Korean cyber actors?

Answer. Response was not received at the time of publication.

Question 5. What can we expect from Iran in the election space going forward?

Answer. Response was not received at the time of publication.

Question 6. Do you think the United States succeeded this election cycle at establishing deterrence against interfering in our elections? Why or why not?

Answer. Response was not received at the time of publication.

Question 7. How do the cyber capabilities of Russia, North Korea, and Iran compare to those of China? How do you expect their capabilities to evolve?

Answer. Response was not received at the time of publication.

Question 8. Please explain the anatomy of a ransomware attack. What are the common threat actors, tactics, and targets? Why is the United States the most targeted country?

Answer. Response was not received at the time of publication.

Question 9. How do expect adversaries such as China, Russia, and Iran to use AI in cyber space in the next 5 years?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR MARK MONTGOMERY

Question 1. Which “Typhoon” concerns you the most and why?

Answer. Both Volt and Salt Typhoon expose the vulnerability of U.S. critical infrastructure to cyber threats from the Chinese Communist Party (CCP) and other U.S. adversaries. While Salt Typhoon’s espionage campaigns against the U.S. telecommunications and intelligence systems pose a significant risk, Volt Typhoon’s pre-positioning within critical sectors presents a more immediate and direct national security threat.

In military terms, Volt Typhoon is operational preparation of the battlefield. Its activities enable the CCP to potentially disrupt or disable essential systems at will, this could be used to disrupt the rail, aviation, and port systems that enable U.S. military mobility and causing societal chaos. Such adversarial pre-positioning would never be tolerated in the physical or kinetic domains, and the same standard must apply to cyber space.

The lack of a strong deterrence strategy invites adversaries to attack the U.S. homeland in cyber space with little fear of retaliation, while the absence of a comprehensive recovery plan leaves the Nation vulnerable to long-term economic and national security consequences. Washington must take decisive action to prevent future cyber attacks through deterrence by denial and resilience, strengthening our defenses to prevent adversary access while ensuring rapid recovery from cyber intrusions. Simultaneously, Washington must enforce deterrence by punishment, im-

posing swift and severe consequences on Beijing to make clear that aggression in the cyber domain carries a high cost.

Question 2. Given reporting indicates Salt Typhoon has been in systems for at least 2 years, does it surprise you that the Government found them first? Why or why not?

Answer. It is not surprising that the U.S. Government, rather than the private sector, discovered Salt Typhoon. Over the years, the Cybersecurity and Infrastructure Security Agency (CISA) has significantly improved its threat-hunting capabilities to detect and respond to cyber threats. These capabilities need to be preserved and built upon.

Meanwhile, CISA has also made strides in public-private collaboration and intelligence sharing, but persistent challenges allow adversaries to remain undetected. This underscores the urgent need for a real-time intelligence-sharing platform like the Joint Collaborative Environment (JCE). The JCE would serve as a centralized hub for exchanging cyber threat information between the Government and the private sector, reducing blind spots that adversaries could exploit. Crucially, this information exchange must occur at the speed of data. The JCE would enable informed decision making and effective response measures by ensuring that both the Government and private-sector leaders have timely, actionable intelligence.

To fully operationalize CISA's role as the National Coordinator as Congress intended, and as outlined in National Security Memorandum 22, Congress must empower CISA to leverage its strong relationships with the private sector and its cyber defense capabilities through the JCE to detect and mitigate future cyber campaigns before they cause serious harm.

Question 3. What can we expect from Iran in the election space going forward?

Answer. The United States does not appear to have publicly imposed costs on Iran for launching aggressive malign influence campaigns targeting the 2024 U.S. elections. Iran created websites targeting minority demographics in swing States, and its most egregious and aggressive campaign was a hack-and-leak operation targeting the Trump campaign. Iran stole sensitive information from the Trump campaign and tried to use it to disparage the campaign and cost Trump the election.

While the Biden administration imposed some limited sanctions on Iran for this activity, this was primarily a name-and-shame operation. But Iran feels no shame. In fact, the lack of forceful response has likely emboldened Iran, and so we can expect to see similar operations in future election cycles or Iran may try to attempt to influence other U.S. policy decisions. In addition, Iran might seek to doxx election officials or incite protests, as it has in its malign influence campaigns targeting the United States in the past.

Question 4. Do you think the United States succeeded this election cycle at establishing deterrence against interfering in our elections? Why or why not?

Answer. There are two categories of election interference: conventional cyber attacks and foreign malign influence. In both cases, the United States succeeded in thwarting adversarial efforts.

Over the past few years, CISA has built important partnerships with State and local officials to provide critical cybersecurity knowledge and information to help secure election infrastructure. These relationships—as well as the activities of local law enforcement—are crucial to ensuring the integrity of U.S. elections against adversarial operations in cyber space. CISA's election cybersecurity efforts must continue.

At the same time, U.S. efforts to counter malign influence were also successful. FDD covered this in a December 2024 research memo, *America Resilient in the Face of Aggressive Foreign Malign Influence Targeting the 2024 U.S. Elections*. Foreign adversaries launched influence campaigns targeting our elections, but they failed at least in part because of efforts within the intelligence community and Federal civilian Executive branch agencies to quickly identify and debunk foreign malign influence operations. Taking down campaigns and raising public awareness are crucial to deny U.S. adversaries benefits of their malign influence campaigns. It is also important to impose costs. If adversaries can continue to target the United States with malign influence campaigns and suffer no consequences, there will be no reason for them to cease launching these low-cost and potentially high-impact operations.

Question 5. What are the barriers to greater investment in cybersecurity and how can we incentivize or work with organizations to overcome those barriers?

Answer. A major barrier to greater investment in cybersecurity is the wide-spread perception that it is a “cost sink” rather than an essential component of business continuity and day-to-day operations. Many organizations prioritize short-term financial gains over long-term resilience, often underestimating cyber risks until they experience a breach first-hand. As a result, investments in upgrading legacy systems are frequently delayed, leaving infrastructure vulnerable to exploitation by

malicious actors. At the same time, duplicative regulations and inconsistent cybersecurity standards across industries create confusion and compliance burdens, further discouraging proactive investment.

To overcome these challenges, businesses must recognize cybersecurity as an enabler for operational success rather than a discretionary expense. This shift can be encouraged through incentives such as tax credits, liability protections for companies that adopt strong security measures, and clear articulation of the benefits of compliance. Additionally, harmonizing Federal cybersecurity regulations to establish clear, enforceable standards and providing accessible resources for businesses—particularly small and mid-sized enterprises—will help drive sustained investment in stronger, more resilient systems.

Question 6. You have conducted cyber exercises in Taiwan and Ukraine. What challenges and strengths did you observe that we should consider in the United States?

Answer. FDD's tabletop exercise in Taiwan revealed that—unlike a cross-strait invasion or military blockade, many CCP cyber actions did not “trip” any redlines in Washington or among allies. The largely stealthy nature of cyber-enabled economic coercion meant that the United States was caught flat-footed as Taiwan faced increasing pressure to acquiesce to Beijing's demands. The United States must not let this precarious position continue. In short, Washington and its allies and partners must develop, exercise, test, and calibrate responses to economic and cyber campaigns, or else Washington's reactions to adversarial activity in the gray zone will always be too slow. I met with Taiwan's President Lai this week and he certainly understands the risk of this cyber-enabled economic warfare and is working to address it, but acknowledges there is critical role for allies and partners (like the United States, Japan, Australia, and Korea) to play.

The United States should consider the following from the exercises in Taiwan and Ukraine:

Expand Defensive Cyber Capacity.—Ukraine provides lessons for Taiwan on the importance of robust cyber defense. Over the better part of a decade, Ukraine has built a highly-skilled cyber workforce. Quick defensive actions by these experts and the U.S. companies who provide cybersecurity services to Ukraine meant that the initial Russian cyber operations were thwarted and remediated. Taiwan similarly needs a highly-effective cyber workforce. Washington should help Taiwan establish partnerships with international technology and cybersecurity firms to protect the integrity of Government and private-sector networks.

Develop an Interagency Playbook of Options to Counter Adversaries in the Gray Zone.—The U.S. Government should develop a new interagency playbook with options for countering China and other U.S. adversaries in a crisis short of war. This playbook should cut across traditionally stove-piped authorities and develop responses that combine cyber, economic, military, legal, and diplomatic levers. Rather than being subject to the crisis of the moment, the playbook should have options that are pre-vetted and reviewed by agency counsels. Periodic crisis planning exercises should test and refine playbook options. This pre-planning and rehearsing will reduce the time to respond to a crisis while also allowing a framework for long-term planning. This approach would ensure that senior U.S. officials have options they can execute rapidly if China or other U.S. adversaries attempt to change the status quo.

Increase Interoperability with Key Partners.—Washington should work to align its interagency playbook with expected allied and partner responses. The United States should exercise the playbook options with key partners and expand other exercises to increase interoperability. For example, Washington should engage in extensive cyber-crisis response planning with Japan and Taiwan, to include testing the ability to defend against a large-scale cyber attack. Exercises should also increase the ability of States to work together in high-pressure situations that emerge from gray zone aggression by U.S. adversaries. For example, the United States could conduct convoy exercises with Japan, Taiwan, and others to demonstrate and expand the ability to escort commercial shipping (such as Liquid Natural Gas (LNG) vessels) during a crisis.

Explore Novel, Indirect Ways to Support Partners Under Siege.—The United States should explore novel, indirect ways of supporting a partner under siege. This includes working with partners to develop mechanisms to utilize private-sector capabilities. This can help Taiwan avoid a readiness trap where it responds to every hostile act in the gray zone. For decades, commercially-owned and -operated contract vehicles have supported intelligence collection and logistics, offering risk- and cost-reducing ways of countering gray zone activity. For Taiwan, increasing maritime and cyber domain awareness helps reduce the CCP's coercive potential. The better the intelligence, the more calibrated Taiwan, the United States, and partner

nations can be. The United States should work with Taiwan and other key partners to explore a common vehicle to fund counter-gray zone activity, including surveillance, cyber defense, and even air-to-air refueling and logistics. This vehicle would make defense dollars go further and bring in private-sector innovation.

Question 7. How do expect adversaries such as China, Russia, and Iran to use AI in cyber space in the next 5 years?

Answer. In the next 5 years, U.S. adversaries will likely use AI to further areas of non-kinetic national power. For example, China is using AI to enhance its biotechnology sector, for mundane uses like enhancing its health care industry through more efficient data collection and analysis to much more concerning projects like exploring military applications of gene editing. Russia is likely to continue using AI to disseminate disinformation and propaganda as well as for scaling and automating cyber attacks. Meanwhile, Iran—currently considered a second-tier cyber actor but conducting increasingly sophisticated operations—is likely to use AI also for its information and influence operations, accelerating and scaling their operations to impact a wider surface in Israel, the United States, and beyond.

Already U.S. adversaries are beginning to use AI tools to help plan and execute cyber attacks and influence operations. A recent report from Google explained that China and Iran used its AI platform Gemini to research socially divisive issues to use in influence campaigns while Russia used it to develop the equivalent of a marketing strategy for its influence operations. Even criminal ransomware groups are beginning to use AI to develop more effective operations and avoid detection by network defenders.

To prevent AI from enabling more dangerous adversarial activity, the U.S. Government will need to work with private companies to help them enhance their cyber and physical security around key elements (such as model weights) and enhance their detection of malign activity. Meanwhile, Washington should continue to work with its allies to develop and enforce export controls on key enabling technologies to restrict the computing power and sophistication of AI platforms built by authoritarian countries.

Question 8. Looking forward to the next 5 years, what emerging cyber threats keep you up at night?

Answer. Over the next 5 years, the most pressing cyber threats will likely continue to be attacks targeting U.S. critical infrastructure, particularly sectors essential to military mobility and national resilience. U.S. adversaries are engaged in operational preparation of the battlefield, holding U.S. infrastructure at risk so that they might disrupt or disable services at the time of their choosing.

Ports, rail networks, and airports—vital for military deployments and global supply chain stability—are already prime targets for adversaries seeking to cripple logistics, thwart U.S. power projection, and destabilize the global economy. Meanwhile, lifeline sectors, such as food supply chains, water systems, health care, and education networks remain dangerously exposed to ransomware and cyber attacks. These attacks could disrupt food distribution, poison water supplies, paralyze hospitals, and threaten the safety of children in schools. These attacks will not only cripple essential services but also endanger lives and destabilize communities across the Nation.

Compounding these risks, cyber-enabled influence operations will likely intensify unless the U.S. Government does something to stop them. U.S. adversaries are and will likely continue spreading malign narratives through a variety of mediums to advance their interests, including sowing societal divisions and creating chaos in both peacetime and wartime.

Without investments to strengthen critical infrastructure resilience, enforce cybersecurity standards, and counter digital influence operations, these threats will escalate—exposing the country to severe disruption, economic instability, and a full-scale national security crisis.

QUESTION FROM HONORABLE GABE EVANS FOR MARK MONTGOMERY

Question. There are concerns about both state-sponsored actors and criminal actors targeting taxpayer-funded Government benefits. In 2022, a Chinese-backed hacker group stole at least \$20 million in U.S. COVID relief benefits. More recently, State and local governments, including those in my State of Colorado, have contended with increasingly sophisticated cyber tactics that target vulnerable beneficiaries of programs such as SNAP, Medicare, and Medicaid.

What tactics are threat actors using to target Government benefits, and what are the threat actors' aims?

Answer. Phishing and business email compromise are the most common tactics employed in breaches into Government agencies. For example, in 2023, hackers

breached Department of Health and Human Services systems, stealing \$7.5 million in civilian grant money. In these attacks, the hackers used spear phishing, a targeted form of phishing to lure specific individuals—in this case, Government employees—into providing access to grantees' accounts.

Cyber criminals seeking financial gain are likely to continue conducting these attacks. Federal civilian Executive branch agencies need better cybersecurity and should implement best practices like using complex passwords and multi-factor authentication. They should also be trained on detecting phishing campaigns and to not open emails from unsafe senders.

This type of basic cyber hygiene can reduce the threat of criminal attacks. Federal agencies, however, must also contend with nation-state threats who could use successful attacks on Federal and State governments to undermine the faith of the American people in their democratic institutions. The efforts of the Cybersecurity and Infrastructure Security Agency to work with other Federal partners as well as State, local, Tribal, and territorial governments are crucial to detecting and thwarting both criminal and nation-state campaigns.

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR BRANDON WALES

Question 1. Which “Typhoon” concerns you the most and why?

Answer. A specialized group within the Chinese military (the People’s Liberation Army), publicly known as Volt Typhoon due to Microsoft’s naming practices, poses the most significant threat to the United States. Their targeting of critical infrastructure in the United States provides Beijing with the ability to disrupt the United States along two fronts: (1) military operations and (2) essential civilian functions. Beijing views this threat against the United States as a powerful deterrent against our military, which relies on networked communication systems between our military assets. Furthermore, publications from the Academy of Military Sciences in Beijing indicate Chinese strategists believe attacking civilian critical infrastructure would degrade American morale and make it less likely that the United States would intervene on behalf of Taiwan in a future conflict.

Question 2. What lessons should CISA take from the discovery of Salt Typhoon to strengthen its role as the Sector Risk Management Agency (SRMA) of the communications sector?

Answer. The discovery of the so-called Salt Typhoon campaign (attributed to actors linked to the Chinese Ministry of State Security) reveals critical cybersecurity failures in the communications sector, where nation-state actors exploited multiple supply chain vulnerabilities in Cisco, Ivanti, Fortinet, and Microsoft software. A key lesson from this campaign is that telecom providers are unevenly implementing even basic cybersecurity protections, the FCC lacks sufficient authority to require such protections (or has sufficient authority, yet is unable or unwilling to use it), and CISA’s voluntary programs alone are insufficient to meet the challenge of today’s threats. While there may be legitimate business reasons for the telecommunications sector’s current approach (e.g., optimizing for network stability and reliability over security), it is time to reevaluate that approach. Additionally, the attack’s success highlights systemic risks from a small set of dominant infrastructure suppliers, making it clear that both service providers and vendors must be held accountable for securing their products and networks.

To strengthen its role as SRMA, CISA must prioritize policy development with the Office of the National Cyber Director, the Federal Communications Commission and the National Telecommunications and Information Administration at the Department of Commerce to ensure streamlined and harmonized cybersecurity regulations for the communications sector. Furthermore, CISA should identify and mitigate systemic points of concentration (e.g., reliance on widely-deployed Cisco, Ivanti, and Fortinet systems) that serve as high-value targets for adversaries. Finally, CISA should expand its Secure by Design initiative to enforce stronger security commitments from critical infrastructure suppliers. Salt Typhoon demonstrates that national security cannot rely on voluntary compliance alone—CISA must drive stronger regulations, supplier accountability, and systemic risk mitigation to protect U.S. communications infrastructure.

Question 3. Given recent compromises of the communications sector with Salt Typhoon, does the U.S. Government have the right resources to stay ahead of the threat to undersea cables?

Answer. Undersea cables and their on-shore infrastructure are at risk from both physical and cyber threats at various locations, with responsibility for their protection and resilience spread among Federal, State, local, and private-sector organizations. Nation-state adversaries, such as Russia, believe that undersea cables are unique asymmetric targets given the United States’ reliance on these assets for eco-

conomic and national security. Resources are needed to ensure the United States can meet this challenge, but given the sensitivity of this topic, it is one that is best discussed with cleared U.S. Government officials. However, at a minimum, the United States, working with our allies in Europe and Asia, must continue to invest in resilience of this vital infrastructure—not just in the security of cables, landing stations, and other components, but also the support and repair infrastructure to ensure timely responses to multiple cable cuts or disruptions.

Question 4. What can we expect from Iran in the election space going forward?

Answer. Given that Iran has attempted to influence both the 2020 and 2024 elections, I do not expect them to stop. While their tactics have evolved, they continue to use cyber-enabled influence operations as a means to sow discord and undermine the confidence of the American people in its democratic institutions. The Nation must be prepared for future operations, not just from the Iranians, but from Chinese, Russian, and other actors, as well.

Question 5. Do you think the United States succeeded this election cycle at establishing deterrence against interfering in our elections? Why or why not?

Answer. The United States has not successfully deterred adversaries from attempting to influence the electorate in our elections, as evidenced by exposed Russian and Iranian efforts in the 2024 cycle. Foreign efforts to interfere in U.S. elections have seen an evolution in tactics, away from technical attacks on election administration itself, to hack-and-leak operations and paying social media influencers. These tactics are cheap, easy to obfuscate, and below the threshold that would typically trigger a significant national-level response. Accordingly, it is arguable that the United States has meaningfully deterred direct technical interference in the administration of our elections, by a mix of system-level hardening, national-level resilience (including training, resourcing, and paper ballots), as well as direct messaging to adversaries.

Question 6. CIRCIA requires covered entities to report ransom payments within 24 hours of making it. Do you think this reporting requirement will help the U.S. Government's ability to reduce the frequency of, or mitigate the damage from, ransomware attacks? Why or why not?

Answer. CIRCIA's 24-hour ransom payment reporting requirement could enhance collective defense by giving CISA and law enforcement faster, more accurate threat intelligence and a clearer picture of ransomware activity. This speed may allow quicker efforts to disrupt criminal operations, track funds, and warn other organizations. However, concerns remain: attackers often operate globally and remain elusive, many organizations may underreport out of fear or unawareness of the reporting requirement, and the requirement is inherently reactive rather than preventive. Ultimately, although this mandate provides a useful tool for the Government to reduce damage from ransomware, its overall effectiveness will depend on robust enforcement, resource allocation, and holistic cybersecurity practices.

Question 7. Why is the health care system uniquely vulnerable to ransomware attacks, and what non-regulatory measures can we take to secure our health care system?

Answer. The health care system shares many common characteristics of other "target-rich, cyber-poor" parts of our critical infrastructure: legacy technology; complex networks; and underfunded or nonexistent cybersecurity capabilities. The biggest challenge most parts of the health care system have is funding. Notwithstanding the current policy prioritization to reduce both Government spending and the regulatory state, cybersecurity grants for technology and cybersecurity expertise to small hospitals and clinics would be the most effective non-regulatory measure we could take.

Question 8. From your perspective, what do you see as the barriers to wide-spread Federal adoption of cutting-edge AI tools?

Answer. Cloud-based and third-party AI solutions must navigate a gauntlet of security and compliance standards—FedRAMP, CMMC, NIST 800-53, DISA SIG—each designed to ensure resilience against cyber threats but adding months, if not years, to the approval time line. Every piece of software (and in many cases the supporting infrastructure and personnel) must be scrutinized, penetration-tested, and certified before it can even touch a Government system . . . Unlike commercial AI models trained on publicly-available data, AI for national security systems must be built on information that can't simply be uploaded to a cloud instance or shared across agencies. Strict governance policies dictate who can access, process, and analyze this data, creating significant hurdles for AI integration. AI models that rely on cloud training often find themselves at odds with security policies designed to limit exposure. Even within on-premises environments, stringent access controls slow the data pipeline, making it difficult to train AI in real time.

Many of the Federal agencies' existing cybersecurity tools were built in an era before AI-driven automation was even a consideration. While AI would absolutely provide a much-needed force multiplier—automating threat hunting, accelerating incident response, and reducing alert fatigue—it often requires extensive custom development to bridge the gap between old and new. Congress, working with the new administration and industry, should conduct a rapid study of steps that could be taken to reduce the bureaucratic process around current IT approvals regimes, accelerating IT modernization, reducing costs, increasing competition and innovation, and ultimately delivering better solutions to citizens.

Question 9. Looking forward to the next 5 years, what emerging cyber threats keep you up at night?

Answer. I am concerned by the possibility that LLMs and AI models will empower a new class of low-skilled hackers, effectively democratizing commodity-level cyber criminal capabilities. Currently, much discussion and research on the impacts of AI to offensive cyber techniques focus on already-advanced actors using the technology to improve their operations. However, these actors are already successful at achieving their goals, so while they may be able to move faster, the overall impact will likely be limited.

Poor quality hackers, often called “script kiddies”, are best known for using pre-made tools to conduct attacks. They are, at best, using copy and paste on their computers to carry out their attacks. As LLMs improve, these unskilled actors who may have extreme ideologies gain better cyber attack skills.

QUESTION FROM HONORABLE GABE EVANS FOR BRANDON WALES

Question. There are concerns about both state-sponsored actors and criminal actors targeting taxpayer-funded Government benefits. In 2022, a Chinese-backed hacker group stole at least \$20 million in U.S. COVID relief benefits. More recently, State and local governments, including those in my State of Colorado, have contended with increasingly sophisticated cyber tactics that target vulnerable beneficiaries of programs such as SNAP, Medicare, and Medicaid.

What tactics are threat actors using to target Government benefits, and what are the threat actors' aims?

Answer. The tactics that adversaries use against public-sector entities are often the same ones they use against all potential targets, namely, weaknesses in widely-adopted technology platforms and systems, and poor cybersecurity practices, such as poorly-configured applications. Often threat actors will target public benefit systems for financial gain. As a result, it is absolutely essential that Federal agencies participate in, and Congress appropriate funds for, efforts like the CISA Continuous Diagnostics and Mitigation (CDM) program, which provides technology to Federal civilian departments and agencies allowing them to reach a baseline of cybersecurity protections.

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR KEMBA WALDEN

Question 1. Which “Typhoon” concerns you the most and why?

Answer. Volt Typhoon. Volt Typhoon has no espionage purpose, rather the intent of the intrusion is to hold our critical infrastructure at risk to deter U.S. involvement in a conflict between China and Taiwan. We need a more defensible and resilient infrastructure to deter and defeat these threats. That means a strong Cybersecurity and Infrastructure Security Agency (CISA), operational collaboration among overlapping cyber defenders, and strengthened public-private operational collaboration.

Though Volt Typhoon concerns me most, Salt Typhoon is also concerning given the infiltration into the backbone of our digital ecosystem. We need to explore which telecommunications vulnerabilities Salt Typhoon exploited to determine cyber operational priorities for improving the resilience of our telecommunications infrastructure. Reinstating the important work of the Cyber Safety Review Board will produce meaningful recommendations for improvements.

Question 2. Given recent compromises of the communications sector with Salt Typhoon, does the U.S. Government have the right resources to stay ahead of the threat to undersea cables?

Answer. No. The U.S. Government needs more resources to stay ahead of the threat to undersea cables. Of the 60 cable-laying ships world-wide, only 2 are registered and owned by a U.S. entity. That is a supply chain vulnerability that demonstrates the lack of resources the United States has in rebuilding submarine cables, should physical or cyber threats disable the connectivity of the lines. Congress established the Cable Security Fleet of 2 vessels capable of installing, maintaining, and repairing submarine cables as part of the National Defense Authorization Act

for Fiscal Year 2020.¹ Congress should consider amending this law to authorize and appropriate additional cable vessels for the Cable Security Fleet to stay ahead of the threat to undersea cables. The U.S. Naval Institute recommends that the U.S. maintain a Cable Security Fleet of 6 vessels.²

The United States should consider a deterrence strategy that imposes costs on vessels that destroy or otherwise damage undersea cables. Although the internet can route through different undersea cables, the scenario in which Pacific cables are damaged, compromised, or destroyed, and all internet traffic is then routed through China becomes increasingly likely—further threatening the safety and security of Americans' data. The U.S. Government should study the approach taken by Finland in protecting undersea cables in the Baltic Seas from damage. In December 2024, the Finnish authorities seized an oil tanker that was suspected of severing an undersea cable in Finnish waters. There have been several such incidents in recent months where ships drag or drop their anchors, severing this vital infrastructure. While countries take the time to investigate to determine whether incidents are accidental or intentional, governments should seek severe consequences for severing undersea cables.³

Question 3. What can we expect from Iran in the election space going forward?

Answer. Iran continues to attempt to compromise U.S. election systems. And their tactics and techniques continue to improve. With the emergence of AI-powered cyber threats and increasing sophistication of cyber attacks, Iranian cyber threats to election infrastructure will increase in scale and sophistication.⁴ We must have a robust defense of our critical infrastructure to defend against and deter this active threat.

Question 4. Do you think the United States succeeded this election cycle at establishing deterrence against interfering in our elections? Why or why not?

Answer. Yes. The United States has been successful in establishing deterrence through defense against interfering in our elections.

Attacks on our democracy erode the safety and security of our Nation. Whether foreign or domestic in origin, these attacks are strategic, coordinated efforts to undermine both the consent of the governed and the legitimacy of our Government in fulfilling its duty to secure our inalienable rights. This problem is not merely a technical one requiring a technical response, nor is it simply a matter of disinformation defense; our adversaries are using every tool at their disposal to erode our security. Although we have responded to attacks on the networks that comprise our election infrastructure, adversaries also foster distrust in democratic principles, making us less safe and secure. Currently, there is no common vision or collective approach to securing our democracy beyond securing our elections. This calls for “all hands on deck.” The call is urgent because if not vigorously addressed it undermines the ability of the United States to lead the free world by example.

Securing our democracy and democratic institutions, including our election process, is a shared responsibility involving individuals, the private sector, State and local governments, the Federal Government, and international organizations. The secure administration of elections is not a partisan political endeavor—it is a core principle of a representative government. It is a joint mission with a common cause. To defend against adversaries that seek to attack our democratic processes and to deter them from doing so in the first place requires a collective approach. The following elements are part of a roadmap to secure elections:

First, the Cybersecurity and Information Sharing Act of 2015 (CISA 2015) protects private-sector owners and operators of the infrastructure underpinning our election systems from adverse consequences from sharing cyber threat indicators and defensive measures amongst themselves. Specifically, Congress authorized private-sector entities to share this information without fear of violating antitrust laws or disclosure of this information through FOIA and State sunshine laws. Moreover, CISA 2015 enabled the private sector to voluntarily share information with State and local government entities that administer elections and the Federal Government entities that provide technical assistance to help protect election systems. CISA 2015 will expire at the end of September if Congress does not reauthorize this foundational enabler of securing our critical infrastructure.

In addition to protecting companies that take defensive measures and share cyber threat information, CISA 2015 also authorizes private companies to monitor their

¹ 6 U.S.C. § 53202.

² “To Secure Undersea Cables, Take Lessons from the British Empire’s All-Red Line.” Available *To Secure Undersea Cables, Take Lessons from the British Empire’s All-Red Line/Proceedings—July 2024 Vol. 150/7/1,457*.

³ *Severing of Baltic Sea Cables Was ‘Sabotage,’ Germany Says—The New York Times*.

⁴ *Exclusive/Chinese and Iranian Hackers Are Using U.S. AI Products to Bolster Cyberattacks—WSJ*.

own networks, or those of their customers upon authorization and written consent, for cybersecurity purposes. The private sector's ability to monitor their own networks and, with permission, the services provided to legislatures or election-sensitive individuals contributed to the success of ensuring that U.S. elections are secure. Private companies played a crucial role in detecting and mitigating cyber threats, thereby enhancing the overall security of the election infrastructure.

Second, the U.S. Government's designation in 2017 of election infrastructure as part of the Government Facilities sector is key to securing our election system. This enables Government agencies, including the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), to designate resources to defend the infrastructure.

Third, CISA and the FBI, for nearly a decade now, have built durable relationships with both parties in every State and territory, and with State secretaries and elections directors. These deep relationships are pivotal in assisting the States to understand their elections infrastructure and deploy the State resources necessary to defend them. This year, CISA provided 10 additional election security advisors across the country and cross-training over 100 physical security inspectors on election infrastructure.⁵ This increased depth and collaboration ensured that State and local election officials were well-prepared to handle the potential cyber and physical threats to election infrastructure and maintain the integrity of the election process.

These efforts must be continuous to keep pace with the evolution of the threats to our election systems. We need robust cyber defenses and increased resilience measures. Sustained investments in election security, cybersecurity, and commitments to election resilience measures are essential elements to increasing the resilience and success of our elections.

Question 5. A growing number of threat groups are targeting operational technology (OT). Why and how are adversaries targeting these systems?

Answer. Adversaries often infiltrate systems by exploiting the convergence of information technology (IT) and OT networks that occurred as organizations sought to improve efficiency and remote monitoring capabilities. Common tactics include compromising vulnerable remote access points, exploiting unpatched legacy systems, and leveraging social engineering to gain initial access to connected IT networks.

State-sponsored threat actors target these systems to establish persistent access for potential disruption during times of conflict, as demonstrated by attacks on power grids, water treatment facilities, and industrial control systems. Criminal groups also target OT environments for ransomware operations, recognizing that the critical nature of these systems creates pressure for organizations to pay. The disruption of Colonial Pipeline in 2021 exemplifies how disrupting OT can have cascading effects across critical infrastructure sectors and in our communities.

The motivation for targeting OT systems stems from their high-impact nature and inherent vulnerabilities. These systems control physical processes in energy production, manufacturing, and critical infrastructure, making them attractive targets for actors seeking to cause wide-spread disruption or establish strategic leverage. The complexity of updating or replacing these systems, combined with their round-the-clock operational requirements, often leaves security gaps that adversaries can exploit. Additionally, many OT systems use proprietary protocols and legacy technologies that weren't designed with modern cybersecurity threats in mind, making them particularly vulnerable to sophisticated attacks that can bypass traditional IT security controls.

Question 6. Which international partnerships do you view as essential to securing cyber space?

Answer. The Department of State Bureau of Cyberspace and Digital Policy (CDP) is chief among the partnerships the United States needs to resource, invest in, and engage to catalyze international partnerships across the globe to secure our shared digital ecosystem. Through CDP, the United States maintains critical cyber partnerships across the world, including with:

NATO and EU

Our relationships with NATO allies and the European Union serve as foundational partnerships for cyber threat intelligence sharing and coordinated incident response. American enterprises operate and sell services in countries that are members of NATO and the European Union. The European Union's Network and Information Security (NIS) Directive framework represents a crucial space in which the United States and the National Institute of Standards and Technology (NIST) can work to establish common security standards and cross-border incident response protocols. Additionally,

⁵*Defending Democracy: The PROTECT2024 Chapter in Election Infrastructure Security/CISA.*

- Germany, as the largest economy in Europe, plays a pivotal role in these partnerships, contributing significant resources and technical expertise to collaborative cybersecurity initiatives.
- France's recent announcement of \$112 billion in investments in artificial intelligence infrastructure increases the opportunity for future collaboration and partnership across Europe.⁶
- Estonia stands out as a key technological leader for cybersecurity innovation.⁷ Estonia's pioneering e-governance systems and experience defending against significant cyber attacks have made it an invaluable partner in developing shared defensive capabilities. Estonia's expertise in digital public services and cyber resilience provides important models for secure digital transformation.

Asia

Counterbalancing strategic competitors like Russia and China will require partnerships with their neighbors, including Singapore, India, and Japan, who remain crucial allies in the security of that continent.

- *Singapore.*—Singapore is a critical technological leader in the Asia-Pacific region, enabling innovation in cybersecurity technologies and shared defensive capabilities. This partnership is strategically valuable given Singapore's position as a technological hub near China, allowing for coordinated regional approaches to cybersecurity challenges in Southeast Asia.
- *India.*—India stands as a pivotal partner in Asia, contributing significant strategic and technological capabilities. As one of the world's largest democracies, India's partnership is invaluable in maintaining stability and countering regional threats. India's advanced IT sector and growing defense industry enhance collaborative efforts in cybersecurity and defense. India's role in regional security dynamics is critical given its strategic location and increasing economic clout.
- *Japan.*—Japan represents another essential partnership in Asia, contributing advanced technological capabilities and strategic positioning. This relationship is particularly important given Japan's economic significance and its role as a counterbalance to Chinese influence in the region. Cooperation with Japan strengthens the broader Indo-Pacific cybersecurity framework.

Latin America/Western Hemisphere

Western Hemisphere partnerships, including the Five Eyes intelligence alliance and deepening commercial ties across shortened semiconductor and global supply chains, strengthen our national security. Partnerships with nations in Latin America and the Western Hemisphere are essential, as these regions experience rapid digital transformation. The relationship with Costa Rica deserves special mention, particularly following Secretary Rubio's recent productive visit. Strengthening these hemispheric partnerships helps establish cyber capacity-building programs and technical assistance that strengthen global cyber resilience and counterbalance against adversaries like China and Russia, who seek footing in Latin and North America.

Additionally, working through multilateral forums like the United Nations Group of Governmental Experts (UN GGE) and the Internet Governance Forum (IGF) allows the United States to shape international cyber norms and standards while promoting a free, open, and secure internet. These diverse partnership channels, coordinated through diplomatic engagement, create an interconnected framework of allies and partners essential for addressing transnational cyber threats and promoting stability in cyber space.

Question 7. Do you agree that cyber defenders have the upper hand with AI? If yes, how do we ensure that the United States maintains that advantage?

Answer. Yes. The development and ingenuity across the AI technology stack are incredible. Take, for example:

AI-enabled managed detection and response (MDR) platforms that leverage AI/ML to provide cyber defenders scalable detection and automation.⁸ The AI/ML sustains 24/7 security monitoring and response for cloud, hybrid, and on-prem environments together with threat intelligence and customization. AI also enables cyber defenders to transform an enterprise's capacity to protect itself from the constant threat of cyber attacks by leveraging AI/ML capabilities to take data from a customer's existing security stack and more efficiently identify and mitigate threats. Customers using MDR platforms benefit from AI-assisted auto-remediation, increasing the

⁶France's answer to Stargate: Macron announces AI investment.

⁷Cyber-security-in-Estonia-2024.pdf.

⁸See, for example, *Leading Managed Detection & Response (MDR) Security Services/Expel*.

speed and scale of incident detection ahead of point product notifications and automating alert analysis, prioritization, and remediation.

Cyber defenders can also leverage an AI Security platform to provide model-agnostic, centralized, and scalable security, observability, and control across all AI models.⁹ The AI Security category delivers a comprehensive suite of solutions that accelerate trust and governance to enterprise and government adoption of AI and machine learning. This use of AI to scan, alert, and protect systems against internal and external risks in real time through dashboards provides full auditability, traceability, and attribution for cost, content, and user engagement. With API integration, AI Security platforms allow companies to efficiently deploy security smoothly into their networks and allow the user to secure their data and future-proof their data security standards when deploying large language models (LLMs).

Virtual content moderators can also leverage AI moderation agents—backed up by real human judgment—to combat cyber crime.¹⁰ Models use captions, audio, and OCR (optical character recognition) context to analyze visual content in the context it appears. Then, by simultaneously analyzing multiple signals, the ML technology can understand videos and images and flag content that opposes the platform’s policies and terms of use, enabling users to undertake more proactive moderation and mitigation against illegal or harmful content, including child sexual abuse material.

Digital watermarking solutions can also protect and authenticate digital assets using forensic watermarks.¹¹ This technology converts the pixels of digital media, including videos and images, into a digital signature to ensure authenticity. With the ability to turn any image into an invisible QR-code, using state-of-the-art photographic steganography and forensic watermarking technology, these solutions enable businesses to protect their digital intellectual property from leaks and misuse, and decrease the amount of counterfeit content out in the digital ecosystem. These solutions provide content provenance, increase digital authenticity, ensure copyright, and permit the rapid vetting and validation of those materials.

AI can also catalyze Security Operation Center (SOC) security information and event management (SIEM) systems.¹² By helping SOC’s make decisions and triage events and alerts at AI speed rather than human speed, SOC’s can rapidly defend networks against increasingly sophisticated threat actors. With AI acting as the security analyst’s assistant, SOC analysts can swiftly sift through the noise that system alerts generate, eliminate false positives, and provide focus-limited staff on the issues that matter for network security. The ability to leverage AI agents to check security alerts by gathering data across multiple sources and types of data (labeled and unlabeled) enriches the alert and highlights the few alerts that need analyst attention. Using LLMs to provide analysts with easy-to-read outputs that include the reason data summarized with recommendations on the next steps to fix the alert uses AI for good.

Finally, an AI for IT operations platform can deliver a significant improvement in end-user experience, response speed, security, and gains to organizational resilience and productivity with a SaaS operating model.¹³ By building AI agents with a human in the loop to displace the human-intensive efforts of IT outsourcing providers or traditional help-desk employees, AI does more with less. A typical company has 1 IT support person per 75 employees. With the deployment of an AI for IT operations platform, IT staff can scale their work and dramatically improve service quality and response time. With a core AI engine and large language models (LLMs), these solutions can turn all IT support into seamless conversations, and it will be integrated into a company’s existing tech stack to proactively identify and remediate issues versus adding to the ticketing queue for an IT professional.

We need more of these solutions out in the marketplace and, as importantly, the ability of the Federal Government to invest in, buy, and distribute these best-in-class solutions before the cyber defenders lose the advantage.

QUESTION FROM HONORABLE GABE EVANS FOR KEMBA WALDEN

Question. There are concerns about both state-sponsored actors and criminal actors targeting taxpayer-funded Government benefits. In 2022, a Chinese-backed hacker group stole at least \$20 million in U.S. COVID relief benefits. More recently, State and local governments, including those in my State of Colorado, have con-

⁹ See, for example, *Secure AI at Inference* / CalypsoAI.

¹⁰ See, for example, *Unitary Virtual Agents/AI BPO for customer, marketplace, and safety operations*.

¹¹ See, for example, *Forensic Watermarking for Digital Media/StegAI*.

¹² See, for example, *embed security/turn down the security noise*.

¹³ See, for example, *IT Help Desk Services/Fixify*.

tended with increasingly sophisticated cyber tactics that target vulnerable beneficiaries of programs such as SNAP, Medicare, and Medicaid.

What tactics are threat actors using to target Government benefits, and what are the threat actors' aims?

Answer. Threat actors are stealing money meant for Government benefits, including the benefits distributed under the Supplemental Nutrition Assistance Program (SNAP). The United States Department of Agriculture distributes SNAP benefits through electronic benefit transfer (EBT) payment cards. In many States, these cards still use magnetic strip technology and have not been updated to use the more secure chip technology used in common bank-issued credit cards. Bank-issued credit cards maintain compliance with PCI-DSS standards, which recommend chip technology, among other things. The magnetic strips on EBT cards are inherently less secure and not currently subject to similar security standards. And therefore, threat actors are more easily able to use the magnetic strip to skim or clone EBT cards.

In December 2023, Congress authorized the USDA to issue promulgate rules requiring State agencies to establish measures by December 2024 to prevent benefits from being stolen.¹⁴ Further, Congress authorized reimbursements to victims of this crime limited to only 2 months of the money allotted to the household and replacement of stolen benefits can occur no more than twice per year.¹⁵ However, this provision expired in December 2024, leaving victims with no Federal reimbursement. Last year, Members of Congress introduced the Enhanced Cybersecurity for SNAP Act of 2024 which would amend the Food and Nutrition Act of 2008 to include specific cybersecurity improvements in connection with EBT cards.¹⁶ By updating the EBT benefit fraud prevention provisions of title 7, Congress could reduce vulnerabilities commonly exploited by threat actors against Government benefits.



¹⁴ 7 U.S.C. § 2016a(a).

¹⁵ 7 U.S.C. § 2016a(b)(2).

¹⁶ Wyden, Fetterman, Cassidy and Bipartisan Members of Congress Introduce Enhanced Cybersecurity for SNAP Act to Secure Food Benefits Against Hackers and Thieves/U.S. Senator Ron Wyden of Oregon.