

SHAPING THE FUTURE OF CYBER DIPLOMACY: REVIEW FOR STATE DEPARTMENT REAUTHOR- IZATION

HEARING

OF THE

SUBCOMMITTEE ON EUROPE

BEFORE THE

COMMITTEE ON FOREIGN AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

April 29, 2025

Serial No. 119-14

Printed for the use of the Committee on Foreign Affairs



Available: <http://www.foreignaffairs.house.gov>, <http://docs.house.gov>, or <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

60-593PDF

WASHINGTON : 2025

COMMITTEE ON FOREIGN AFFAIRS

BRIAN J. MAST, Florida, *Chairman*

MICHAEL T. McCAUL, Texas	GREGORY W. MEEKS, New York, <i>Ranking Member</i>
CHRISTOPHER H. SMITH, New Jersey	BRAD SHERMAN, California
JOE WILSON, South Carolina	GERALD E. CONNOLLY, Virginia
SCOTT PERRY, Pennsylvania	WILLIAM R. KEATING, Massachusetts
DARRELL ISSA, California	AMI BERA, California
TIM BURCHETT, Tennessee	JOAQUIN CASTRO, Texas
MARK E. GREEN, Tennessee	DINA TITUS, Nevada
ANDY BARR, Kentucky	TED LIEU, California
RONNY JACKSON, Texas	SARA JACOBS, California
YOUNG KIM, California	SHEILA CHERFILUS-McCORMICK, Florida
MARIA ELVIRA SALAZAR, Florida	GREG STANTON, Arizona
BILL HUIZENGA, Michigan	JARED MOSKOWITZ, Florida
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa	JONATHAN L. JACKSON, Illinois
WARREN DAVIDSON, Ohio	SYDNEY KAMLAGER-DOVE, California
JAMES R. BAIRD, Indiana	JIM COSTA, California
THOMAS H. KEAN, JR, New Jersey	GABE AMO, Rhode Island
MICHAEL LAWLER, New York	KWEISI MFUME, Maryland
CORY MILLS, Florida	PRAMILA JAYAPAL, Washington
RICHARD McCORMICK, Georgia	GEORGE LATIMER, New York
KEITH SELF, Texas	JOHNNY OLSZEWSKI JR, Maryland
RYAN K. ZINKE, Montana	JULIE JOHNSON, Texas
JAMES C. MOYLAN, Guam	SARAH McBRIDE, Delaware
ANNA PAULINA LUNA, Florida	BRADLEY SCOTT SCHNEIDER, Illinois
JEFFERSON SHREVE, Indiana	MADELEINE DEAN, Pennsylvania Q04
SHERI BIGGS, South Carolina	
MICHAEL BAUMGARTNER, Washington	
RYAN MACKENZIE, Pennsylvania	

James Langenderfer, *Majority Staff Director*

Sajit Gandhi, *Minority Staff Director*

SUBCOMMITTEE ON EUROPE

KEITH SELF, Texas, *Chairman*

MICHAEL T. McCAUL, Texas	WILLIAM KEATING, Massachusetts,
JOE WILSON, South Carolina	T3Ranking Member K
MARK GREEN, Tennessee	DINA TITUS, Nevada
YOUNG KIM, California	JIM COSTA, California
WARREN DAVIDSON, Ohio	GABE AMO, Rhode Island
ANNA	JULIE JOHNSON, Texas
AULINA LUNA, Florida	SARAH McBRIDE, Delaware

Michael Koren, *Subcommittee Staff Director*

C O N T E N T S

REPRESENTATIVES

Opening Statement of Subcommittee Chairman Keith Self	Page 1
Opening Statement of Subcommittee Ranking Member William Keating	2

WITNESSES

Statement of Annie Fixler, Director, Center on Cyber and Technology, Foundation For Defense of Democracies	4
Prepared Statement	7
Statement of Latesha Love-Grayer, Director, International Affairs and Trade, U.S. Government Accountability Office	19
Prepared Statement	21
Statement of Theodore Nemeroff, Co-Founder and Vice President for Data and Compliance, Verific AI.	37
Prepared Statement	39

APPENDIX

Hearing Notice	60
Hearing Minutes	62
Hearing Attendance	63

QUESTIONS FOR THE RECORD

Questions for the Record submitted to Ms. Latesha Love-Grayer from Rep. Gabe Amo	64
--	----

SHAPING THE FUTURE OF CYBER DIPLOMACY: REVIEW FOR STATE DEPARTMENT REAUTHORIZATION

Tuesday, April 29, 2025

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON EUROPE,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:19 p.m., in room 2200, Rayburn House Office Building, Hon. Keith Self (chairman of the subcommittee) presiding.

Mr. SELF. The Subcommittee on Europe will come to order. The purpose of this hearing is to discuss the subcommittee's areas of jurisdiction for the State Department authorization, which includes the Bureau of Cyberspace and Digital Policy.

I now recognize myself for an opening statement.

OPENING STATEMENT OF CHAIRMAN KEITH SELF

I want to welcome members and witnesses to the subcommittee on Europe's second hearing on State Department reauthorization. Today, the subcommittee will be exploring the role of the State Department in cyber and technology matters, and how such policies might align with U.S. national security interests and foreign policy objectives. In particular, we will be examining the work of the Bureau of Cyberspace and Digital Policy, or CDP. Across the globe malicious cyber attacks are conducted by State and nonState actors against the United States and its allies, including from the People's Republic of China, from cyber criminals scamming individuals out of their savings to large scale state-sponsored attacks from America's adversaries. U.S. Government entities and citizens are increasingly under siege. For years, PRC-supported hackers have buried deep into critical infrastructure, including water transportation networks and energy systems.

According to the 2025 annual worldwide threats assessment of the U.S. IC, intelligence community, the PRC remains the most active and persistent cyber threat to U.S. Government private sector and critical structure networks. Beijing's campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracking publicly as volt typhoon, or it more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of the PRC's capability to compromise U.S. infrastructure.

Russia also poses a significant cyber threat with its efforts to compromise sensitive targets for intelligence collection and to preposition access to U.S. critical infrastructure. In addition to Beijing and Moscow, Tehran has demonstrated an increasing willingness to carry out aggressive cyber operations to the security of U.S. networks and data.

Furthermore, Pyongyang's cyber program presents a highly capable and maturing threat, including an approach to launder and cash out cryptocurrency from the United States and other victims to fund its nefarious activities. As cyber becomes a growing battlefield for criminal networks and malignant actors, the State Department must be ready to meet the challenge. The U.S. is not facing these real and growing threats alone, it took cooperation with our allies and our partners. The U.S. will continue to work to combat and align cyber activities from PRC, Iran, North Korea and Russia.

Since the recent establishment of CDP, it has played a role in the U.S. response to a major ransomware campaign in Costa Rica that disrupted critical services. In particular, CDP, alongside other Federal partners, work to strengthen Costa Rica's cyber defenses against attacks from malicious actors threatening the security of both our countries. It has also worked to identify strategic opportunities to leverage partner resources to further U.S. strategic objectives through subsea cable projects in the Pacific Islands.

Such efforts ensure that the Pacific Islands rely on trusted, primarily American businesses for their internet connectivity while also countering the PRC's influence in the strategically imported region. On the other hand, the Department of State agreement on a cybercrime U.N. treaty that conflicted with CDP policy lead and recommendations begs the question of the actual authority wielded by CDP. This hearing should lead us toward conclusions on how to improve CDP efficiency and effectiveness in this vital area of national interest and security.

As we move through this reauthorization process, the experience and insights from today's witnesses will help inform this subcommittee on the State Department's cyber diplomacy role in addressing these increasingly important challenges.

I look forward to hearing your testimony and recommendations. The chair now recognizes the ranking member, the gentleman from Massachusetts, Mr. Keating, for any statement he may have.

OPENING STATEMENT OF RANKING MEMBER WILLIAM KEATING

Mr. KEATING. Thank you, Mr. Chairman and to our witnesses for being here today. For years, bipartisan members of this committee have recognized the necessity for the State Department to take on the important task of cyber diplomacy. In 2021, the Biden administration announced the creation of the Bureau of Cyberspace and Digital Policy, CDP, with bipartisan support and the Department of State Authorization Act of 2022 authorized the CDP Bureau into statute, an important step in recognizing the need for robust and comprehensive approach to cyber diplomacy.

With the CDP bureau established in statute, its work in conjunction with this committee to lead the State Department's diplomatic cyberspace and cybersecurity efforts encompassing both hard secu-

rity and economic policy. As our adversaries, Russia, China, Iran and North Korea, each take different approaches to undermining U.S. actions in cyberspace, bolstering U.S. cyber capability through a strong CDP bureau is more important than ever.

The CDP bureau has worked to advanced U.S. interest in cyberspace across multiple lines of effort. For example, following the 2022 ransomware attack in Costa Rica by a Russian-linked cyber crime group, the CDP bureau provided swift, decisive, support to Costa Ricans and their authorities to bolster the country's digital defenses and resiliency. This emergency support was critical to ensure that a partner in our own hemisphere was able to effectively respond to an unprecedented attack. Similarly, the State Department worked to strengthen Ukraine cyber defenses in the midst of Russia's full-scale, illegal invasion of the country through the digital connectivity cybersecurity partnership program, a joint venture by the Department of USAID.

These are just a few examples of the CDP bureau's important work to bolster our allies and partners while promoting American values and security in cyberspace.

While I appreciate the opportunity to talk about an important bureau, which is long maintained by partisan support, it is unfortunately clear that neither this majority nor the Trump administration has any interest or intent to engage constructively on a reauthorization of the State Department.

Last week, Secretary Rubio unveiled a proposed reauthorization plan for the State Department without any meaningful consultation with Congress. Reorganization would decimate the Department's cyber policy tools by splitting it in half. CDP's economic structures would be moved under the economic family of the bureau and CDP's hard security offices would be placed in a new emerging threats bureau. This move will create exactly the duplication and the waste this administration says it seeks to avoid. Even more concerning, it deprioritizes a crosscutting issue that needs to be tackled holistically and at the highest levels.

Our witnesses here today and many experts in the field have all pointed out the importance of capacity building in cyberspace and maintaining and recruiting the skills required for qualified cyber diplomacy workforce.

Unfortunately, rather than invest in capacity building in places like Costa Rica and Ukraine, the Trump administration has slashed the U.S. foreign assistance budget and illegally eliminated USAID, a chief implementer with capacity-building programs.

At the same time, GAO and Ms. Love-Grayer, they found out that nonpartisan report, that while CDP is currently staffed and fully operational, it needs to train existing staff and hire more people to meet its growth plans. Rather than seeking to recruit and train staff, the Trump administration has attacked and politicized the Federal workforce, leaving a legacy of destruction and indeed distrust.

Finally, rather than listen to the advice of experts, consult with industry professionals and engage with the State Department, this committee has effectively served as a rubber stamp for the administration's destructive actions.

Ms. Fixler, you concluded in an article on March 17th the capacity building program, including those implemented by USAID, are not merely altruistic endeavors, they advance critical U.S. interest. Ms. Love-Grayer, your nonpartisan 2024 GAO report concluded that the State Department provides foreign assistance to strengthen partner capacity and to promote cyber norms to achieve U.S. cyber policy objectives.

Mr. Nemeroff, your testimony points out that a well-placed cybersecurity foreign assistance project can make all the difference in leveling the playing field for our companies and private investments in countries that still deeply respect U.S. tech leadership. Yet rather than invite administration witness here from the CDP bureau to testify on the effectiveness of the bureau's programming or implement the advice of experts like our witnesses here today, the chair of the full committee and many of my major majority colleagues have already wholeheartedly endorsed the administration's reorganization plans. This is a troubling abdication of the oversight responsibilities of this committee, and an elimination of the Article I authority of this Congress.

I look forward to the testimony of our witnesses here today. I would strongly urge my majority colleagues to listen to what they have to say, work to reauthorize the State Department in a way that serves the interest of the American public, and move this important issue to the foreign front.

I yield the balance of my time.

Mr. SELF. Other members of the committee are reminded that opening statements may be submitted for the record.

We are pleased to have a distinguished panel of witnesses before us today on this important topic. Ms. Annie Fixler, Director of Center on Cyber and Technology at the Foundation for Defense of Democracies; Ms. Letesha Love-Grayer, Director of International Affairs and Trade at the U.S. GAO; and Mr. Theodore Nemeroff, co-founder and Vice President for Data and Compliance at Verific AI.

This committee recognizes the importance of the issues before us and is grateful to have you here to speak with us today. Thank you. Your full statements will be made part of the record. And I will ask each of you to keep your spoken remarks to 5 minutes in order to allow time for our member questions.

I now recognize Ms. Fixler for your opening statement.

STATEMENT OF ANNIE FIXLER

Ms. FIXLER. Thank you, Chairman Self, Ranking Member Keating, and distinguished members of the committee, on behalf—

Mr. SELF. Would you check your mic, or get closer to it?

Ms. FIXLER. Sorry.

Mr. SELF. Pull it close to you.

Ms. FIXLER. Better?

Mr. SELF. Try it.

Ms. FIXLER. Thank you, Chairman Self, Ranking Member Keating, and distinguished members of the committee, on behalf of the Foundation for Defense of Democracies, thank you for inviting me to testify today.

For years, on a bipartisan basis, members of this committee pushed the State Department to better organize itself to defend U.S. national security in cyberspace. Two and a half years after creating the Bureau of Cyberspace and Digital Policy, this committee must assess its performance, expand its successes and address its shortcomings. This hearing is particularly timely, given the Department's proposed reauthorization which appears to put its cybersecurity efforts at risk and contradict congressional guidance to integrate cybersecurity and digital economy efforts.

In my written testimony, I describe the successes the bureau has been able to achieve because of this integration. I would like to take this opportunity to summarize the threat we face and the role States cyber bureau should play.

Every day malicious cyber operators sitting in remote corners of the world attack our critical infrastructure. Across energy transportation and communication systems, China has prepositioned destructive capabilities. Beijing is prepared to use crippling cyber attacks to induce societal panic and interfere with our ability to project power.

During the Biden administration, we issued stern warnings but failed to deter Chinese aggression. Trump administration officials and Members of Congress have rightfully articulated that our Nation needs to go on the offense and punish those who use cyberspace to do us harm. And we need better defense to deny our adversaries their objectives.

The cyber bureau plays a critical role in both. Over the course of its short tenure it has demonstrated it understands these priorities and can execute the mission.

Congress tasked the bureau with managing a unique cyber assistance fund because lawmakers recognized it took far too long for us to respond to incidents overseas that might cascade and hit our homeland. Now in as little as 2 days, the bureau can airdrop expertise into partner countries.

The Department bolsters allied law enforcement capability to investigate cyber crime and prosecute the offenders and convinces those same allies and partners to join us when we call out bad behavior.

The first step to getting our allies and partners to impose costs on China is for them to agree that a cyber attack has occurred and that Beijing is to blame. The bureau helps allies and partners proactively build cyber resilience. On this, our strategic priorities are clear: We need the countries that we fight with and through to have resilient infrastructure. Resilience buys America time to deploy a range of policy responses. Had Ukraine succumbed to Russian cyber attacks, Washington could not have provided the lethal aid that has helped Kyiv substantially degrade the military capabilities of a leading U.S. adversary.

Last summer, FDD led a tabletop exercise in Taiwan, exploring Chinese cyber enabled economic warfare against the island. In the game, the thing that gave Beijing the greatest pause was not U.S. countermeasures, but an assessment that Taiwan could withstand the attack. If China believed that Taiwan could survive, it would refrain from attacking in the first place, lest Taiwan's strengths reveal the CCP's limits. Resilience has a deterrent power all its own.

But building the resilience of allies and partners will be a Sisyphean task if the telecommunications infrastructure underpinning all of it is built by China.

The U.S. military does not have operational security if Beijing is listening on the line. In the CHIPS Act, Congress tasked and funded efforts at State to secure information communications technology. The cyber bureau is wisely using its portion on undersea cables in the Indo-Pacific.

When Congress created the bureau, lawmakers rightfully articulated that its head must be a principal cybersecurity policy official in the Department. It also needs permanent staff billets so that the funding Congress appropriate is spent wisely and efficiently. There is a battle underway in cyberspace. Without a robust cyber bureau, we will not win.

Thank you for inviting me to testify today. I look forward to your questions.

[The prepared statement of Ms. Fixler follows:]

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Foreign Affairs Subcommittee on Europe

Shaping the Future of Cyber Diplomacy:

Review for State Department Reauthorization

ANNIE FIXLER

Director and Research Fellow
Center on Cyber and Technology Innovation
Foundation for Defense of Democracies

Washington, DC
April 29, 2025



www.fdd.org

Introduction

Chairman Self, Ranking Member Keating, and distinguished members of the committee, thank you for inviting me to testify today.

The United States is in daily conflict with adversaries that use cyber as a weapon. Beijing, Moscow, Pyongyang, and Tehran all recognize that they can challenge American leadership and undermine our national security without having to face down the American military — the most powerful and capable force in the world. Instead, their operators sit in remote corners of the globe and attack our critical infrastructure and that of our allies and partners.

Chinese officials have admitted as much, according to reporting in *The Wall Street Journal*.¹ Beijing, in essence, warned Biden administration officials that their cyber operatives are prepared — in the words of the U.S. intelligence community — to use crippling cyberattacks to induce “societal panic” to interfere with Washington’s ability to project power abroad.² Across U.S. and allied energy, transportation, and communications systems, China has pre-positioned disruptive and destructive capabilities. Chinese operatives have burrowed deep into telecommunications networks across the United States, Europe, and the Indo-Pacific to spy on government officials — including President Donald Trump and Vice President JD Vance — as well as everyday Americans.³

During the Biden administration, Washington issued stern warnings and imposed economic sanctions on individuals and companies involved in malicious cyber operations. This failed to deter Chinese aggression. Trump administration officials and members of Congress have rightfully said that our nation needs to go on the offense and create the conditions for deterrence in cyberspace. We need better offense to punish our adversaries for their malign cyber activity. And we need better defense and resilience to deny our adversaries their objectives.

The State Department has a critical role to play in both efforts. The department helps strengthen the cyber resilience of our allies and partners to reduce risks to U.S. forces. And it corrals those same allies and partners to impose costs on those who use cyberspace to do us harm.

Members of this committee have long articulated the importance of State’s role in defending U.S. national interests and security in cyberspace. For years, on a bipartisan basis, members worked with the State Department and pushed it to better organize itself for the mission and

¹ Dustin Volz, “In Secret Meeting, China Acknowledged Role in U.S. Infrastructure Hacks,” *The Wall Street Journal*, April 10, 2025, (<https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb>)

² U.S. Office of the Director of National Intelligence, “Annual Threat Assessment of the U.S. Intelligence Community,” March 2025, Page 12. (<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>)

³ Jonathan Greig and Martin Matishak, “At least 8 US telcos, dozens of countries impacted by Salt Typhoon breaches, White House says,” *The Record*, December 4, 2024. (<https://therecord.media/eight-telcos-breached-salt-typhoon-nsc>)

consolidate its cyber, technology, and emerging threats expertise within a single bureau.⁴ In December 2022, as a result of the vision and leadership of this committee, Congress created the Bureau of Cyberspace and Digital Policy at the State Department with the cross-cutting authorities necessary to lead cyber diplomacy.⁵

Two and a half years later, this committee has an opportunity to 1) assess the performance of the bureau, 2) build upon and expand its successes, and 3) address its shortcomings. Congress should use this moment to ensure the bureau is adequately resourced and given proper authority within the department to help our partners become more resilient in cyberspace, to help them recover from attacks and prosecute the perpetrators, and to guide the long-term investments necessary to build the communications infrastructure that our nation and its warfighters need.

Over the course of its short tenure, the cyber bureau has demonstrated it understands these priorities and can effectively and efficiently execute the mission. Its experts recognize that our national security demands that our partners and allies be able to withstand and quickly recover from cyber assaults. Where the bureau has fallen short, it has often been the result of other equities in the department overriding the bureau's determinations. The bureau needs control over cyber dollars and the staff to manage their deployment. And it must be situated within State's security pillar so that those dollars are spent not on economic development overseas but rather on the security of the United States and the resilience of our partners and allies.

Cyber Resilience of U.S. Allies and Partners

Partner and allied cyber resilience ensures the United States has maximum flexibility to respond to adversarial aggression. Exercises and real-world incidents bear this out.

Last summer, FDD experts led a tabletop exercise in Taiwan focused not on the most dangerous scenarios — a cross-strait invasion or blockade — but rather the most likely: aggressive Chinese economic and cyber measures designed to break Taiwan's societal resilience and force the island to acquiesce to reunification with the mainland under the Chinese Communist Party (CCP).⁶ In the game, no amount of U.S. diplomatic or economic pressure affected the CCP's calculus. What did give Beijing pause, however, was an assessment that Taiwan could withstand the coercion. If the CCP believed that Taiwan could outlast and potentially even thrive despite China's gray zone coercion, the CCP might refrain from launching its cyber-enabled economic warfare campaign in the first place lest Taiwan's strength reveal the CCP's limits. Resilience has a deterrent power all its own.

After the game, the China team also revealed what they feared most — that the U.S. team would rally its partners and allies in Asia and Europe to join Washington's economic pressure

⁴ Mark Iozzi, "Bolstering America's Cyber Diplomacy Capabilities," *Oral remarks at the Foundation for Defense of Democracies*, February 24, 2021. (<https://www.fdd.org/events/2021/02/24/bolstering-americas-cyber-diplomacy-capabilities>)

⁵ James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 STAT. 3898, §9502. (<https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>)

⁶ Craig Singleton, Rear Adm. (Ret.) Mark Montgomery, and Benjamin Jensen "Targeting Taiwan: Beijing's Playbook for Economic and Cyber Warfare," *Foundation for Defense of Democracies*, October 4, 2024. (<https://www.fdd.org/analysis/2024/10/04/targeting-taiwan>)

campaigns. But rallying allies and partners takes time. Economic sanctions also take time to have an effect. So, resilience buys America the time necessary to consider and deploy a broader range of policy responses. Had Ukraine succumbed to the Russian cyberattacks against its government systems in the lead-up to Moscow's February 2022 invasion,⁷ the United States would not have had time to provide the lethal assistance that has helped Ukraine — in the words of my colleagues at FDD — “substantially degrade[] the second-leading conventional military threat to the United States.”⁸

The State Department's cyber bureau has a key role to play, helping allies and partners build this cyber resilience.⁹ The State Department helps our partners and allies train cybersecurity personnel to defend critical infrastructure¹⁰ and develop national cyber strategies so that those countries can prioritize strengthening their own defenses. These programs are immensely popular around the world because they provide the technical expertise our partners lack.¹¹ When State requested proposals from its interagency partners and embassies on where to allocate the Cyberspace, Digital, and Related Technologies Fund established by Congress, the bureau received hundreds of ideas. But as any cyber professional or business executive knows, cyber funds are limited. We must prioritize where we deploy State's limited cyber resources.

Until now, that prioritization has been haphazard. Despite the creation of State's cyber bureau, much of the funding for what is known as cyber capacity building comes from regional programs within the department. A Government Accountability Office (GAO) report warned two years ago that as a result of this structure, State and other federal agencies lacked a comprehensive, coherent assessment of their impact.¹² Too often, the decisions on where and how to spend funds were driven by regional considerations without the unique expertise of State's cyber professionals.

The Biden administration's Joint Strategic Plan for the State Department, for example, outlined several cyber objectives but placed the cyber bureau in charge of only some of them.¹³ USAID and other State Department bureaus made programmatic decisions independently without

⁷ Chris Riotta, “U.S. cyberspace ambassador lays out technology's role in geopolitical contests,” *NextGov/FCW*, February 2, 2023. (<https://www.nextgov.com/cybersecurity/2023/02/us-cyberspace-ambassador-lays-out-technologys-role-geopolitical-contests/382538>)

⁸ Ryan Brobst and Bradley Bowman, “Arsenal of Democracy: Arming Taiwan, Ukraine, and Israel While Strengthening the U.S. Industrial Base,” *Foundation for Defense of Democracies*, April 7, 2025. (<https://www.fdd.org/analysis/2025/04/07/arsenal-of-democracy>)

⁹ Rear Adm. (Ret.) Mark Montgomery and Annie Fixler, “Building Partner Capabilities for Cyber Operations,” *Foundation for Defense of Democracies*, July 27, 2023. (<https://www.fdd.org/analysis/2023/07/27/building-partner-capabilities-for-cyber-operations>)

¹⁰ David DiMolfetta, “US taps IBM for 5-year deal to boost European, Eurasian allies' cyber posture,” *NextGov/FCW*, July 17, 2024. (<https://www.nextgov.com/cybersecurity/2024/07/us-taps-ibm-5-year-deal-boost-european-eurasian-allies-cyber-posture/398090>)

¹¹ Nathaniel C. Fick, “US Leadership in Tech Diplomacy: A Conversation with Ambassador Nathaniel C. Fick,” *Oral remarks at the Hudson Institute*, June 21, 2023. (<https://www.hudson.org/events/us-leadership-tech-diplomacy-conversation-ambassador-nathaniel-c-fick>)

¹² U.S. Government Accountability Office, “Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime,” March 2023, page 14. (<https://www.gao.gov/assets/gao-23-104768.pdf>)

¹³ U.S. Department of State, U.S. Agency for International Development, “Joint Strategic Plan FY 2022-2026,” March 2022. (https://www.state.gov/wp-content/uploads/2022/03/Final-State-USAID-FY-2022-2026-Joint-Strategic-Plan_29MAR2022.pdf)

coordinating with other departments, U.S. allies, or the private sector, all of whom have their own cyber resilience programs and incident response and recovery capabilities.

The problem persists today but can be fixed if State's cyber bureau is given more control over where and how to spend coveted cyber dollars — and the permanent staff billets to manage them. The bureau should be able to direct funding based on America's strategic priorities and the programs that Congress has specifically authorized¹⁴ rather than having internal State Department foreign assistance determinations reallocated these dollars elsewhere.

America's strategic priorities — when it comes to foreign cyber resilience — are straightforward: we need those countries that we fight alongside and fight through to have resilient critical infrastructure.

At FDD, we just published a report exploring the importance of civilian-owned critical infrastructure to military mobility.¹⁵ In the United States, to move service members and military equipment, the Pentagon relies on 18 commercially owned strategic seaports, about 70 civilian-owned airfields, and 40,000 miles of commercially owned rail lines. Private and municipally owned electricity, water, and telecommunications utilities supply our military bases. Reflecting on the findings of the congressionally mandated Cyberspace Solarium Commission, my colleagues and I have urged the federal government to prioritize the cyber resilience of these types of systemically important entities.¹⁶

The United States needs our partners and allies to do the same. While our research so far has focused on U.S. national cyber resilience, my team is beginning a new effort to analyze the intersection of critical infrastructure resilience and military mobility for NATO. But it does not require a deep dive to know that American military bases abroad similarly rely on critical infrastructure owned and operated not by the Department of Defense but by local governments and companies. U.S. military readiness requires reliable, secure infrastructure wherever U.S. forces operate. We need our partners and allies to invest in the resilience of their infrastructure.

With the State Department's cyber bureau at the helm, the federal government can direct resources toward this effort. Some partners will need foreign aid, some will need technical expertise, while many others will simply need State's help brokering agreements with private American companies to supply cybersecurity services. Collectively, these efforts will reduce the risk to U.S. forces and put the fear of American power into our adversaries.

¹⁴ National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 990.

(<https://www.congress.gov/118/plaws/publ31/PLAW-118publ31.pdf#page=856>)

¹⁵ Annie Fixler, Rear Adm. (Ret.) Mark Montgomery, and Rory Lane, "Military Mobility Depends on Secure Critical Infrastructure," *Foundation for Defense of Democracies*, March 27, 2025.

(<https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure>)

¹⁶ Jiwon Ma and Rear Adm. (Ret.) Mark Montgomery, "2024 Annual Report on Implementation: Top 10 Recommendations for the Incoming Administration and Congress," *Cyberspace Solarium Commission 2.0*, September 2024. (https://cybersolarium.org/wp-content/uploads/2024/09/CSC2.0_Monograph_2024AnnualReport_Top10.pdf)

Incident Response and Punishment of the Perpetrators

State Department's cyber bureau also has unique capabilities to rapidly push resources to allies and partners under attack from malicious cyber operators when those attacks pose risks to U.S. national security. Congress specifically created a cyber assistance fund managed by the bureau because lawmakers recognized it was taking far too long for the United States to respond to cyber incidents overseas that might otherwise cascade and hit our homeland.¹⁷ Now, in as little as two days, State Department's cyber bureau can "airdrop" private sector technical expertise into countries in the midst of a significant cyber incident.¹⁸ The bureau has developed the necessary mechanism to effectively and efficiently use the resources it has.

According to press reporting, this past November, State provided this swift and decisive support to mitigate the effects of a potentially catastrophic ransomware attack on the largest oil refinery in Costa Rica.¹⁹ For less than \$500,000, State's cyber bureau provided technical expertise, software, and other support. In a short, 10-day deployment, U.S. experts helped the refinery investigate, remediate, and recover from the incident and harden systems against future attacks. As anyone who has dealt with a cyberattack unfortunately knows, they often take significantly longer and cost orders of magnitude more to remediate. This quick infusion of technical expertise was possible because of prior investments in the country's cybersecurity capabilities.²⁰

Sometimes recovery will be arduous. After Iranian cyber operators destroyed Albanian government systems in July 2022 — putting the country on the brink of a national emergency — the United States poured \$50 million into the country to harden its cyber defenses.²¹ This incident helped inform congressional efforts to create a nimbler cyber assistance mechanism. In cyberspace, the old adage is true that an ounce of prevention is worth a pound of cure. But with the new incident response capabilities and funding mechanisms of State's cyber bureau, Washington can act faster and better stretch a dollar.

The federal government does not have unlimited dollars to spend on incident response. The cyber bureau focuses on major incidents affecting national security priorities — like pushing

¹⁷ Sydney J. Freedberg, Jr., "State Dept wants 'cyber assistance fund' to aid allies and partners against hackers," *Breaking Defense*, April 10, 2023. (<https://breakingdefense.com/2023/04/state-dept-wants-cyber-assistance-fund-to-aid-allies-and-partners-against-hackers>); Eric Geller, "America's cyber ambassador on how to spend \$50 million in foreign aid," *The Record*, April 22, 2024. (<https://therecord.media/cyber-foreign-aid-nathaniel-fick-state-department>); Cyberspace, Digital Connectivity, and Related Technologies (CDT) Fund, 22 U.S.C. Chapter 32, Subchapter II, Part X. (<https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter32/subchapter2/part10&edition=prelim>)

¹⁸ Martin Matishak, "Exclusive: State Department cyber bureau preps funding blitz aimed at boosting allies' defenses," *The Record*, September 24, 2024. (<https://therecord.media/state-dept-preps-funding-blitz-to-boost-cyber-defenses-fick>)

¹⁹ Martin Matishak, "Costa Rica refinery cyberattack was first deployment for new US response program, ambassador says," *The Record*, January 17, 2025. (<https://therecord.media/state-department-falcon-cyber-response-costa-rica-recope>)

²⁰ U.S. Government Accountability Office, "Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities," January 2024, Page 17-18. (<https://www.gao.gov/assets/d24105563.pdf>)

²¹ U.S. Ambassador Yuri Kim, "Remarks at the 'Cyber Security Challenges in Albania' Conference," *Remarks before the Cyber Security Challenges in Albania Conference*, February 7, 2023. (<https://al.usembassy.gov/remarks-by-u-s-ambassador-yuri-kim-at-the-cyber-security-challenges-in-albania-conference>)

back against Chinese influence in Latin America. Costa Rica has been a key partner in that effort.²² Washington's rapid intervention and the quick recovery of the company also prevented an energy crisis in the country and preempted impacts on global energy markets.

The State Department also helps bolster the law enforcement capabilities of partners and allies to investigate cybercrime and prosecute the offenders. Because legal expertise resides in State's Bureau of International Narcotics and Law Enforcement Affairs (INL), much of this law enforcement work is logically conducted and funded by INL in coordination and partnership with the FBI's cyber legal attachés.²³ The latter are also crucial to joint operations to dismantle cybercriminal enterprises that victimize American companies and American citizens.²⁴

Leveraging the relationships INL and FBI develop, as well as those maintained by technical experts within the Department of Homeland Security (DHS), is essential for Washington's efforts to corral allies and partners into issuing joint attributions of malign cyber activity. As noted, China fears a collective response from the United States and its allies. The first step to getting our partners and allies to impose costs on China is for them to agree that a cyberattack has occurred and that Beijing is to blame.

As the Cyberspace Solarium Commission explained, joint attribution can deter future malicious activity because actors know that bad behavior is more likely to be severely punished. Joint attribution is also a form of burden sharing. When allies and partners join the United States in calling out and punishing bad behavior, they share the "cost and effort associated with activities such as intelligence collection and analysis, attribution, and response actions," the commission concluded.²⁵ State's cyber bureau is well positioned to persuade allies and partners to join our efforts to identify — and punish — the perpetrators of cyberattacks.

Telecommunications Infrastructure: The Long-Term Investment

Building the cyber resilience of allies and partners will be a Sisyphean task if the telecommunications systems underpinning their infrastructure are built by China. Control of this network represents the proverbial high ground in modern warfare.²⁶ The U.S. military cannot operate effectively if its secure communications are not, in fact, secure but instead are being read in real time by operatives in Beijing. As the State Department itself has warned, if the CCP

²² Mathieu Pollet and John Hendel, "The West is on a world tour against Huawei," *Politico*, November 28, 2023. (<https://www.politico.eu/article/west-world-tour-huawei-china-telecom>)

²³ Rear Adm. (Ret.) Mark Montgomery and Annie Fixler, "Building Partner Capabilities for Cyber Operations," *Foundation for Defense of Democracies*, July 27, 2023. (<https://www.fdd.org/analysis/2023/07/27/building-partner-capabilities-for-cyber-operations>)

²⁴ U.S. Federal Bureau of Investigation, "FBI Deploys Cyber Experts to Work Directly with Foreign Partners," *Federal Bureau of Investigation*, October 26, 2016. (<https://www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners>); Rear Adm. (Ret.) Mark Montgomery and Jiwon Ma, "Targeting FBI Budget Makes Us More Vulnerable on Cyber," *The Cipher Brief*, December 1, 2023. (<https://www.thecipherbrief.com/column/cyber-advisor/targeting-fbi-budget-makes-us-more-vulnerable-on-cyber>)

²⁵ U.S. Cyberspace Solarium Commission, "Report," March 2020, Page 46. (<https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf>)

²⁶ Samantha Ravich and Annie Fixler, "The Economic Dimension of Great-Power Competition and the Role of Cyber as a Key Strategic Weapon," *The Heritage Foundation*, October 30, 2019. (<https://www.heritage.org/military-strength-essays/2020-essays/the-economic-dimension-great-power-competition-and-the-role>)

controls “global telecommunications networks or semiconductor supply chains, they have the means to manipulate or disrupt essential services, critical infrastructure, and supply chains with the push of a button.”²⁷

For this reason, during the first Trump administration, the State Department launched the Clean Network initiative to drive China out of U.S. and partner telecommunication infrastructure.²⁸ Congress continued pushing these efforts, establishing and appropriating funds for the International Technology Security and Innovation (ITSI) Fund in 2022.²⁹ Congress dictated that this be used to secure information and communications technology, semiconductor supply chains, and other emerging technology.³⁰ Congress reemphasized this priority again in the FY 2024 National Defense Authorization Act, creating the Digital Connectivity and Cybersecurity Partnership program to reduce American and allied reliance on imports from China for information and communications technology.³¹

While the cyber bureau does not control all of ITSI’s allocations, it is wisely using its portion to prioritize securing undersea cables.³² Both China and Russia are sabotaging these critical communications pipelines, forcing NATO to increase naval patrols in the Baltic and North Seas.³³ At the same time, with its Quad partners — Australia, Japan, and India — the United States established an initiative on cable connectivity and resilience to help protect the very cables China would seek to sever in order to hamper U.S. communication with Taiwan.³⁴

The problem is not only the physical security of the global undersea cable system that carries 95 percent of international communications. China also seeks to gain a significant share of the market for the production and operation of submarine cables. The Federal Communications Commission is rightfully concerned that the use of Chinese components in U.S. submarine cable infrastructure or the ownership of that infrastructure by Chinese state-backed enterprises will

²⁷ “The U.S. Department of State International Technology Security and Innovation Fund,” *U.S. Department of State*, accessed April 16, 2025. (<https://www.state.gov/the-u-s-department-of-state-international-technology-security-and-innovation-fund>)

²⁸ “The Clean Network,” *U.S. Department of State*, accessed April 16, 2025. (<https://2017-2021.state.gov/the-clean-network>)

²⁹ U.S. Department of State, “Fiscal Year 2024 Congressional Budget Justification, Appendix 1: Department of State Diplomatic Engagement,” April 26, 2023, page 79. (<https://www.state.gov/wp-content/uploads/2023/04/FY-2024-CBJ-Appendix-1-Full-Documents-25-April-2023.pdf>)

³⁰ Erin L. Murphy, “Protect, Promote, Secure: Maximizing the International Technology Security and Innovation Fund,” *Center for Strategic and International Studies*, May 15, 2023. (<https://www.csis.org/analysis/protect-promote-secure-maximizing-international-technology-security-and-innovation-fund-0>)

³¹ Jonathan G. Cedarbaum and Matt Gluck, “Cyber Provisions in the FY2024 NDAA,” *Lawfare*, January 22, 2024. (<https://www.lawfaremedia.org/article/cyber-provisions-in-the-fy2024-ndaa>)

³² Martin Matishak, “Exclusive: State Department cyber bureau preps funding blitz aimed at boosting allies’ defenses,” *The Record*, September 24, 2024. (<https://therecord.media/state-dept-preps-funding-blitz-to-boost-cyber-defenses-fick>)

³³ Jack Burnham, “US and allies must get tough on Russia, China’s deep-sea cable sabotage,” *New York Post*, February 26, 2025. (<https://nypost.com/2025/02/26/opinion/us-must-get-tough-on-russia-chinas-deep-sea-cable-sabotage>)

³⁴ “Cable Connectivity and Resilience Centre,” *Australian Government, Department of Foreign Affairs and Trade*, accessed April 22, 2025. (<https://www.dfat.gov.au/international-relations/regional-architecture/quad/cable-connectivity-and-resilience-centre>)

dramatically heighten the risk of espionage or sabotage.³⁵ The State Department's cyber bureau in turn works with allies and partners to similarly protect the security and reliability of global telecommunications infrastructure. For instance, working with Pacific Island nations, State has facilitated relationships with American technology and communications companies and provided seed funding to improve infrastructure supporting U.S. military installations in Hawaii, Guam, and the Indo-Pacific.³⁶ The resulting project boxed out Chinese firms attempting to dominate the telecommunications infrastructure in the region.

These large infrastructure projects are time and capital intensive. They require long-term, consistent investment. These projects have been especially hard hit by cuts to, and inconsistent messaging around, U.S. foreign assistance.³⁷ These projects are often multistep efforts where the bureau provides a small initial investment and lines up important, subsequent commitments from technology companies and other partners, doubling and tripling the overall impact. Freezes do not just delay these projects but derail them. Congress, however, can remedy this challenge by reaffirming America's commitment to secure communications infrastructure.

A much less capital-intensive way that the cyber bureau helps ensure countries use trusted and secure communications equipment is by helping them reform their regulatory landscape to make it easier for U.S. companies to compete. U.S. legal experts help our partners and allies reform their rules so that contracts are not simply awarded to the lowest bidder.³⁸ This matters because Chinese state-backed entities will always underbid U.S. competitors — because Beijing lavishes them with sizable, market-corrupting subsidies. China can order its companies to operate at a financial loss so that the regime gains access and control over key markets. By helping allies and partners create a regulatory environment that assesses bids not just on price but also on security and reliability, the cyber bureau opens the door for U.S. businesses in these markets.

Not just on a bilateral basis, but also in multilateral arenas, the cyber bureau promotes the market-driven approach and counters Beijing's efforts to corrupt international discussions and technical standards bodies to advantage Chinese companies.³⁹ Companies and countries that

³⁵ Rear Adm. (Ret.) Mark Montgomery, Craig Singleton, Jack Burnham, and Annie Fixler, "Review of Submarine Cable Landing License Rules and Procedures To Assess Evolving National Security, Law Enforcement, Foreign Policy, and Trade Policy Risks: Schedule of Application Fees," *Foundation for Defense of Democracies*, April 14, 2025. (<https://www.fdd.org/analysis/2025/04/14/review-of-submarine-cable-landing-license-rules-and-procedures-to-assess-evolving-national-security-law-enforcement-foreign-policy-and-trade-policy-risks-schedule-of-application-fees>)

³⁶ Winston Qiu, "VAKA Cable lands in Tuvalu, the nation's first submarine cable," *Submarine Cable Networks*, December 12, 2024. (<https://www.submarinenetworks.com/en/systems/trans-pacific/vaka/vaka-cable-lands-in-tuvalu>); White House, Press Release, "Fact Sheet: Enhancing the U.S.-Pacific Islands Partnership," September 25, 2023. (<https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/25/fact-sheet-enhancing-the-u-s-pacific-islands-partnership>)

³⁷ Annie Fixler and Johanna Yang, "USAID Cuts Demolish Cyber Assistance to U.S. Allies and Partners," *The Cipher Brief*, March 17, 2025. (https://www.thecipherbrief.com/column_article/usaids-cuts-demolish-cyber-assistance-to-u-s-allies-and-partners)

³⁸ U.S. Government Accountability Office, "Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities," January 2024, Page 19. (<https://www.gao.gov/assets/d24/105563.pdf>)

³⁹ Craig Singleton, "Countering Threats Posed by the Chinese Communist Party to U.S. National Security," *Testimony before the House Committee on Homeland Security*, March 5, 2025. (<https://www.fdd.org/analysis/2025/03/05/countering-threats-posed-by-the-chinese-communist-party-to-u-s->

propose technical standards gain first-mover advantages and can reshape the technology landscape in their favor.⁴⁰ State's cyber bureau has the technical expertise and relationships with companies necessary to defend U.S. interests in international standards setting forums such as the International Telecommunications Union and the International Electrotechnical Commission.

When U.S. engagement in these bodies is directed by career diplomats and not State's cyber experts, however, America sometimes ends up supporting initiatives that run directly counter to U.S. national interests. Last year, the United States voted in favor of a disastrous cybercrime treaty in the United Nations. The treaty reflects Russian and Chinese views of state control of the internet and will do nothing to stop malicious activity in cyberspace.⁴¹ Numerous human rights groups, cybersecurity experts, and technology companies opposed the treaty.⁴² The lead State Department negotiator — hailing not from the cyber bureau but from INL and lacking cybersecurity expertise⁴³ — determined that the United States could not buck consensus and reject the treaty despite its serious flaws.⁴⁴ Washington can use international forums and technical standards bodies to pursue its interests in open, interoperable, and secure internet but only when negotiators have the cyber expertise and backbone to fight for American interests.

Recommendations

When Congress created the Bureau of Cyberspace and Digital Policy, lawmakers rightfully articulated that the head of this bureau must be the “principal cyberspace policy official” in the department.⁴⁵ Congress should review the organization of the bureau and the department to ensure that vision is realized.

[national-security](#)); Emily de la Bruyère, “China’s quest to shape the world through standards setting,” *Hinrich Foundation*, July 13, 2021. (<https://www.hinrichfoundation.com/research/article/trade-and-geopolitics/china-quest-to-shape-the-world-through-standards-setting>)

⁴⁰ Natalie Thompson and Rear Adm. (Ret.) Mark Montgomery, “Strengthening U.S. Engagement in International Standards Bodies,” *Day One Project*, June 2021. (<https://fas.org/wp-content/uploads/2021/06/Strengthening-U.S.-Engagement-in-International-Standards-Bodies.pdf>)

⁴¹ Ivana Stradner, “China and Russia are using the UN to censor the world,” *The Telegraph* (UK), September 1, 2023. (<https://www.telegraph.co.uk/news/2023/09/01/china-xi-jinping-vladimir-putin-united-nations/>); Ivana Stradner, “Biden must rally against a Russia-led UN ‘cybercrime treaty,’” *The Hill*, June 28, 2022. (<https://thehill.com/opinion/cybersecurity/3535621-biden-must-rally-against-a-russia-led-un-cybercrime-treaty/>); Ivana Stradner, “Will a United Nations Cybercrime Treaty Help Russia, Communist China, and Iran Control the Internet?” *New York Sun*, August 22, 2024. (<https://www.nysun.com/article/will-a-united-nations-cybercrime-treaty-help-russia-communist-china-and-iran-control-the-internet/>)

⁴² Jonathan Greig, “UN General Assembly approves cybercrime treaty despite industry backlash,” *The Record*, December 26, 2024. (<https://therecord.media/un-general-assembly-approves-cybercrime-treaty-despite-industry-pushback/>); Tech Accord, Press Release, “Cybersecurity Tech Accord calls for changes to new UN treaty to prevent damage to global security online,” July 29, 2024. (<https://cybertechaccord.org/press-release-cybersecurity-tech-accord-calls-for-changes-to-new-un-treaty-to-prevent-damage-to-global-security-online>)

⁴³ Deborah McCarthy, “UN Cybercrimes Treaty Negotiations,” *U.S. Department of State*, June 27, 2024. (<https://2021-2025.state.gov/briefings-foreign-press-centers/un-cybercrimes-treaty-negotiations>)

⁴⁴ Suzanne Smalley, “UN cybercrime treaty lead negotiator: US will suffer if it doesn’t vote yes,” *The Record*, October 7, 2024. (<https://therecord.media/un-cybercrime-treaty-lead-negotiator-us-must-pass>)

⁴⁵ James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3898, §9502. (<https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>)

1. **Place an assistant secretary at the helm:** This committee recognized the cross-cutting nature of the work that needed to be done and the seniority and authority that its leader must have, settling on an ambassador with the equivalent rank of an assistant secretary and confirmed by the Senate. This is a good option, but as Congress assesses how to make the bureau most effective, it should evaluate whether placing an assistant secretary (confirmed by the Senate) at the helm would provide consistency in the bureaucracy. Whether an ambassador or an assistant secretary, the right structure and seniority of the bureau will help it not only to engage with senior foreign government officials but also to maintain and expand relationships with interagency partners. According to GAO, the bureau maintains formal interagency agreements to “leverage expertise, broaden insights, and develop a whole of government approach to ... capacity building, technical assistance, and training.”⁴⁶ In addition, the bureau regularly and informally collaborates and deconflicts with FBI and DHS and leverages the political and economic officers around the world who receive its cyber training.⁴⁷
2. **Ensure the bureau is positioned within the department’s security mission:** More important than the title of the head of the cyber bureau is the organizational hierarchy. The head should report directly to senior officials in the department and not through layers of deputies and assistant secretaries. The bureau’s mission is security focused rather than economic development. As such, it should report to the undersecretary of arms control and international security rather than the undersecretary for economic growth as proposed in the administration’s new reorganization.⁴⁸ The legislation that codified the bureau did so in large part to consolidate what were then disparate functions and expertise. To remain the principal cybersecurity policy official within the department, the bureau must retain its jurisdiction over international cybersecurity issues.
3. **Resource and staff the bureau for the mission and ensure it can execute that mission:** Congress also must ensure that the bureau itself has the expertise it needs and can deploy the financial resources Congress has directly authorized and appropriated. To do this, the bureau needs permanent staff billets. Moreover, even as the State Department continues its foreign assistance evaluation and reassessment, lawmakers should remind department officials that they expect the bureau to execute the tasks they have dictated. Funding Congress specifically appropriated for cyber programs should be spent wisely, efficiently, and promptly.

In addition to assessing and possibly adjusting the structure and resourcing, Congress should set priorities for the bureau and consolidate cyber dollars under its direction so that it can implement these priorities.

⁴⁶ U.S. Government Accountability Office, “Cyber Diplomacy: State’s Efforts Aim to Support U.S. Interests and Elevate Priorities,” January 2024, Page 18. (<https://www.gao.gov/assets/d24105563.pdf>)

⁴⁷ Eric Geller, “The Tech Crash Course That Trains US Diplomats to Spot Threats,” *Wired*, July 2, 2024. (<https://www.wired.com/story/us-state-department-diplomacy-school>)

⁴⁸ U.S. Department of State, Press Release, “Building an America First State Department,” April 22, 2025. (<https://www.state.gov/building-an-america-first-state-department>)

4. **Consolidate cyber resilience programs, incident response funding, and telecommunications initiatives under State's cyber bureau:** With its focus on securing U.S. cyber leadership abroad, the cyber bureau has the expertise to allocate funding based on Washington's global cyber priorities. Too often in the past, decisions on how to spend funds for cyber capacity building were driven by regional considerations or other foreign assistance priorities that failed to account for global, cyber-specific needs. Congress should ensure that the cyber capacity-building programs it authorizes and funds continue and that they are consolidated under the direction of the cyber bureau so that the State Department can spend its cyber assistance dollars wisely. As part of this effort, Congress should assess whether these programs are funded at the right level or if more funding is necessary to advance U.S. strategic interests.
5. **Let the cyber bureau lead in international forums and technical standards bodies:** Congress tasked the bureau with promoting freedom of speech and religion and encouraging the development and adoption of international cybersecurity and technology standards. To prevent shameful negotiations and votes like Washington's acquiescence to the China- and Russia-backed UN cybercrime treaty, the bureau needs to be able to do its job. Lawmakers should exercise oversight to ensure State understands and abides by congressional intentions.
6. **Prioritize building allied and partner cyber resilience in critical infrastructure:** Building the cyber resilience of our partners' critical infrastructure — particularly ports, rail systems, and air transport systems — protects military mobility for both the host nation and U.S. forces. Other infrastructures — power, water, and telecommunications — are also critical not just to societal resilience but also to U.S. military readiness. Cyber resilience deters malign activity and provides Washington with greater flexibility in how and when we respond to adversarial aggression against partners and allies. The bureau should prioritize cyber resilience programs in countries whose infrastructure is most critical to the U.S. military's ability to fight and win wars. We need to prioritize cybersecurity dollars where it matters most for U.S. strategic interests and where the movement and lethality of our forces depend on secure local critical infrastructure.

Conclusion

This committee understands the critical role that cyber diplomacy plays in national security. That is why lawmakers created the State Department's cyber bureau. But the bureau cannot function without a senior leader at the helm, without the resources and personnel to accomplish the task Congress has set before it, and without the authority to do what needs to be done to secure our digital borders.

As we speak here today, in these hallowed halls, there is a battle underway in cyberspace. Without a robust cyber bureau at the Department of State, we will not win.

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

Mr. SELF. Thank you, Ms. Fixler.

I now recognize Ms. Love-Grayer for your opening statement. Welcome.

STATEMENT OF LATESHA LOVE-GRAY

Ms. LOVE-GRAY. Chairman Self, Ranking Member Keating, and members of the subcommittee, thank you for the opportunity to discuss our work on the Bureau of Cyberspace and Digital Policy known as CDP. As international trade communication and critical infrastructure grow more dependent on cyberspace and digital technology, there is an opportunity to advance U.S. interests in this digital ecosystem. But also an increase in foreign cyber threats. Foreign governments and nonState actors are increasingly using cyberspace as a platform to target critical infrastructure and our citizens, undermine democracies and international institutions and uncut global competition by stealing ideas when they cannot create them. These are among the reasons that GAO has identified information security as a high-risk issue.

In April 2022, State established CDP to lead U.S. Government international efforts to advance our interest in cyberspace, which State defines as cyber diplomacy. Its overarching objectives included building coalitions, strengthening capacity and reinforcing alarms in cyberspace.

State uses two main tools to implement the cyber diplomacy mission, diplomatic engagement and leadership and multilateral and bilateral fora and foreign assistance that provide training and technical assistance to our international partners.

Examples of the diplomatic efforts include engaging with the European Union to develop shared principles in the 6G wireless network. And supporting the negotiation process of the U.N. cybercrime convention, which appropriately, if appropriately ratified, would facilitate international cooperation to combat cyber crime.

As Congress considers State's reauthorization, my statement today is intended to help inform the discussion about the cyber diplomacy efforts and was based primarily on the reports that we have issued between September 2020 and January 2024 related to those efforts.

State's cyber diplomacy efforts have evolved between 2011 and the present. Between 2011 and 2018, State established the Office of the Coordinator of Cyber Issues to lead global diplomatic engagement and developed an international cyberspace policy strategy document among other efforts. In January 2019, Members of Congress introduced the Cyber Diplomacy Act of 2019, which would have established a new office to lead State's international cyberspace efforts and consolidate a range of crosscutting cyber issues.

Later that year, State notified Congress of its intent to establish a bureau that was more narrowly focused on cybersecurity. In September 2020 and January 2021, we assessed these efforts to establish the cyber bureau. We found that it had not involved other Federal agencies that contributed to international cyber diplomacy and the development of its plan and recommended that it do so.

We also found that State had not demonstrated that it had used data and evidence to develop its proposal for establishing the bu-

reau, and therefore, lacked assurance that its proposal would effectively set priorities and allocate resources to achieve those goals. We recommended that it do so.

In response, State consulted other key Federal agencies and its planning and collected data and evidence to inform its approach, which resulted in changes to the final plan for the bureau.

Once the bureau was established, we examined how it was structured to accomplish its goals. CDP contains four units, including the office of the coordinator for digital freedom, international information and communications policy, international cyberspace security, and a strategies program in communications unit. The new consolidated bureau and the appointment of a Senate-confirmed Ambassador at large to lead it elevated cyber issues in State's diplomatic engagement, that Ambassador engaged with various other country senior leaders on advancing cyber goals.

As an example, in August 2023 the Ambassador headed the U.S. delegation to the G-20 digital economy ministerial meeting he highlighted U.S. views and priorities on digital economy topics.

In addition, we reported that CDP status as a bureau provided senior-level support, resources, and involvement, that did not exist before. Although State's efforts to promote cyber diplomacy have evolved, challenges remained. Among them clearly defining CDP's roles and responsibilities across overlapping issuers with other inter, intra and inter agencies that conduct work in cyber diplomacy, especially given the breadth of cyber issues, as well as ensuring that the bureau has sufficient expertise to carry out its goals.

These are among the challenges that the bureau will still need to effectively navigate to lead cyber diplomacy in the future, especially a State considers streamlining its functions and addressing any new priorities of the administration.

Chairman Self, Ranking Member Keating and members of the subcommittee, this concludes my oral statement. I would be happy to take questions at this time.

[The prepared statement of Ms. Love-Grayer follows:]



United States Government Accountability Office

Testimony
Before the Subcommittee on Europe,
Committee on Foreign Affairs, House of
Representatives

For Release on Delivery
Expected at 2:00 p.m. ET
Tuesday, April 29, 2025

CYBER DIPLOMACY

The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests

Statement of Latesha Love-Grayer, Director
International Affairs and Trade

GAO Highlights

Highlights of [GAO-25-108445](#), a testimony before the Subcommittee on Europe, Committee on Foreign Affairs, House of Representatives

Why GAO Did This Study

As international trade, communication, and critical infrastructure grow more dependent on cyberspace and digital technology, the U.S. and its allies face intensifying foreign cyber threats in critical areas. Foreign governments and non-state actors are increasingly using cyberspace as a platform from which to target critical infrastructure and U.S. citizens. This undermines democracies and international institutions and organizations. It also undercuts fair competition in the global economy by stealing ideas when they cannot create them. CDP's mission is to promote U.S. national and economic security by leading, coordinating, and elevating foreign policy on cyberspace and digital technologies.

This statement discusses:

- the evolution of cyber diplomacy at State that led to the eventual creation of CDP, including the status of recommendations GAO made during its creation;
- how the bureau has organized itself to accomplish cyber diplomacy goals and the types of efforts it undertakes; and
- challenges the bureau faces in fulfilling its goals.

This statement is based on three GAO reports related to State's cyber diplomacy programs—[GAO-20-607R](#), [GAO-21-266R](#), and [GAO-24-105563](#). For that work, GAO analyzed State documents and data and interviewed agency officials. For a full list of the reports, see Related GAO Products at the conclusion of this statement.

For more information, contact Latesha Love-Grayer at lovegrayer@gao.gov.

April 29, 2025

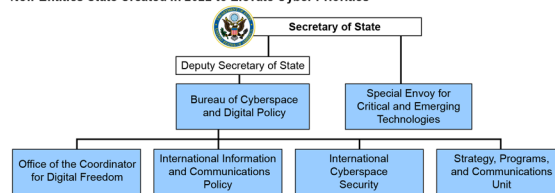
CYBER DIPLOMACY

The Bureau of Cyberspace and Digital Policy's Efforts to Advance U.S. Interests

What GAO Found

The Department of State leads U.S. government international cyber diplomacy efforts to advance U.S. interests in cyberspace. To help achieve those objectives, State established the Bureau of Cybersecurity and Digital Policy (CDP) in April 2022. In doing so, State addressed GAO's recommendations to involve federal stakeholders and use data and evidence in planning for the bureau. State created the bureau to elevate cyberspace as an organizing concept for U.S. diplomacy by consolidating efforts and leadership of cyber-related activities into a single unit. CDP's cyber diplomacy strategic objectives include building coalitions, strengthening capacity, and reinforcing norms.

New Entities State Created in 2022 to Elevate Cyber Priorities



New entities created

Source: GAO based on Department of State documentation (data); Department of State (seal). | GAO-25-108445

In 2024, GAO reported that State conducts a range of diplomatic and foreign assistance activities aligned with U.S. cyber objectives. For example, State works to build coalitions of countries that share U.S. strategic objectives to (1) counter threats to the U.S. digital ecosystem and (2) reinforce global norms of responsible state behavior. CDP leads or coordinates many of these activities for State. For example, CDP rallies countries that share U.S. goals to coordinate policies that advance an open, free, global, interoperable, reliable and secure internet. CDP also facilitates bilateral diplomacy efforts through activities such as interagency whole-of-government cyber dialogues, which involve communication with partner nations.

GAO also reported that CDP faced ongoing organizational challenges, including clarifying roles, hiring staff, and ensuring it had the expertise needed to carry out its goals. Although cyber responsibilities are defined under the new structure, roles remain deliberately shared across government, making clarification an ongoing challenge. CDP was also working to clarify State's role in the interagency process and maintain its lead in cyber diplomacy. CDP officials noted that defining roles across overlapping issues and sustaining internal communication and visibility remain key challenges, especially given the broad scope of cyber issues. Ensuring the bureau has trained staff to carry out its goals may also be a challenge. State must effectively navigate these challenges for CDP to achieve its stated goals.

United States Government Accountability Office

Chairman Self, Ranking Member Keating, and Members of the Subcommittee,

Thank you for the opportunity to discuss our work on the Bureau of Cyberspace and Digital Policy (CDP), which leads, coordinates, and elevates foreign policy on cyberspace and digital technologies for the Department of State. As international trade, communication, and critical infrastructure grow more dependent on cyberspace and digital technology, the U.S. and its allies face intensifying foreign cyber threats in these and other critical areas. Foreign governments and non-state actors are increasingly using cyberspace as a platform for irresponsible behavior from which to:

- target critical infrastructure and U.S. citizens,
- undermine democracies and international institutions and organizations, and
- undercut fair competition in the global economy by stealing ideas when they cannot create them.

Aggressive cyberattacks on civilian infrastructure as well as government systems illustrate this risk. At the same time, the global arena presents positive opportunities for the U.S. to instill key values into the digital ecosystem, including the belief in the potential of digital technologies to promote connectivity, democracy, peace, the rule of law, sustainable development, and the enjoyment of human rights and fundamental freedoms. GAO has designated information security as a government-wide high-risk area since 1997.¹ This high-risk area was expanded in 2003 to include protecting the cybersecurity of critical infrastructure.²

State leads U.S. government international efforts to advance U.S. interests in cyberspace. According to State, these efforts are identified as “cyber diplomacy” activities, which cover a wide range of U.S. interests in cyberspace. These include cybercrime, cybersecurity, digital economy, international development and capacity building, internet freedom, and internet governance. Its cyber diplomacy strategic objectives include building coalitions, strengthening capacity, and reinforcing norms. To help achieve those objectives, State established CDP in April 2022.

¹GAO, *High-Risk Series: An Overview*, [HR-97-1](#) (Washington, D.C.: Feb. 1, 1997).

²GAO, *High-Risk Series: An Update*, [GAO-03-119](#) (Washington, D.C.: Jan. 1, 2003).

As Congress considers State's reauthorization, my statement today is intended to help inform the discussions about State's efforts to advance cyber diplomacy, based on our prior assessments. Specifically, I will discuss the evolution of cyber diplomacy at State that led to the eventual creation of CDP, including the status of recommendations we made during its creation; how the bureau has organized itself to accomplish cyber diplomacy goals and the type of efforts it undertakes; and challenges the bureau faces in fulfilling its goals.

This statement is based primarily on reports published from September 2020 to January 2024 related to State and its cyber diplomacy programs. For those reports, we analyzed State documents and data related to the programs we reviewed, and we interviewed agency officials. We made two recommendations in the reports covered by this statement, both of which State has since implemented.

More detailed information on the objectives, scopes, and methodologies for that work can be found in the issued reports listed in Related GAO Products at the conclusion of this statement. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

State's Cyber Diplomacy Activities Have Evolved

State leads U.S. government international efforts to advance the full range of U.S. interests in cyberspace, which include coordinating with other federal agencies, such as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and the Treasury, to advance the cyber priorities and interests of the nation. State's efforts to advance U.S. interests in cyberspace have evolved over the years, including more recently in response to GAO's recommendations:

- In 2011, State established the Office of the Coordinator for Cyber Issues in the Office of the Secretary to lead the department's global diplomatic engagement on cyber issues and to serve as liaison to other federal agencies that work on cyber issues.
- In 2016, the *Department of State International Cyberspace Policy Strategy* affirmed the elevation of cyberspace policy as a foreign

policy imperative and the prioritization of State's efforts to mainstream cyberspace policy issues in its diplomatic activities.³

- In **2018**, pursuant to Executive Order 13800, State led the development of an international engagement strategy in coordination with other federal agencies to strengthen the U.S. government cooperation with other countries and international organizations to address shared threats in cyberspace.⁴
- In **January 2019**, members of Congress introduced the Cyber Diplomacy Act of 2019, which would have established a new office to lead State's international cyberspace efforts that would consolidate cross-cutting efforts on international cybersecurity, digital economy, and internet freedom, among other cyber diplomacy issues.⁵
- In **June 2019**, State notified Congress of its intent to establish a new bureau that would focus more narrowly on cyberspace security and the security aspects of emerging technologies.

In **September 2020**, we reported on State's plans at that time to establish a cyber bureau.⁶ We found that State had not involved other federal agencies that contribute to international cyber diplomacy in the development of those plans, contrary to leading practices of governmental reform. We recommended that State involve relevant federal agencies in their plans to establish a cyber bureau to obtain their views and identify potential risks.

Taking our recommendation and previous work into consideration, in **May and June of 2021**, State met with senior officials from relevant federal agencies, including the Departments of Defense, Commerce, and Homeland Security as well as officials from the National Security Council

³Department of State *International Cyberspace Policy Strategy*, March 2016. Accessed October 22, 2019. www.2009-2017.state.gov/documents/organization/255732.pdf.

⁴Exec. Order 13800, 82 Fed. Reg. 22391 (May 16, 2017); and Department of State, Office of the Coordinator for Cyber Issues, *Recommendations to the President on Protecting American Cyber Interests through International Engagement*, May 31, 2018. www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf.

⁵*Cyber Diplomacy Act of 2019*, H.R. 739, 116th Cong. (2019). The House of Representatives passed a similar version of the bill during the 115th Congress, see *Cyber Diplomacy Act of 2017*, H.R. 3776, 115th Cong. (2017).

⁶See GAO, *Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau*, GAO-20-607R, (Washington, D.C.: Sept. 22, 2020).

and the Office of the National Cyber Director. During these consultations, State obtained these agencies' views and identified risks, implementing our recommendation.

In our **January 2021** report, we found that State had not demonstrated that it had used data and evidence to develop its proposal.⁷ Without data and evidence, State lacked assurance that its proposal would effectively set priorities and allocate appropriate resources for the bureau to achieve its intended goals. We recommended that State use data and evidence to justify its current proposal or any new proposal to establish a cyber bureau.

In response to our recommendation, State conducted:

- qualitative internal assessments to identify staffing and skills gaps, and
- evidence- and data-based reviews with internal and external stakeholders over a months-long process to develop proposals to establish the bureau.

Implementing data and evidence-based reviews helped to ensure that State's final proposal would achieve its intended results.

State's Reform Effort Has Helped to Elevate Cyber Diplomacy Goals

State Established a New Bureau to Prioritize Cyber Diplomacy

In April 2022, State established a new Bureau of Cyberspace and Digital Policy (CDP) with a mission to address national security challenges, economic opportunities, and implications to U.S. values associated with cyberspace, digital technologies, and digital policy. State created CDP, headed by a Senate-confirmed Ambassador-at-Large, to elevate cyberspace as an organizing concept for U.S. diplomacy by consolidating efforts and leadership of cyberspace-related activities into a single unit.

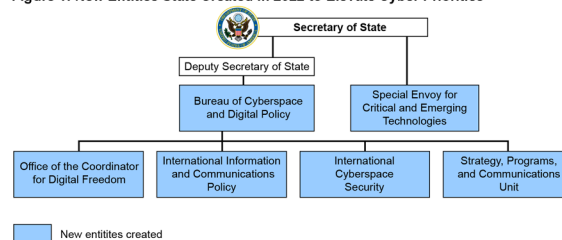
⁷GAO, *Cyber Diplomacy: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies*, [GAO-21-266R](#) (Washington, D.C.: Jan. 28, 2021).

The U.S. Ambassador-at-Large for Cyberspace and Digital Policy serves as the principal cyberspace policy official at State and advisor to the Secretary on cyber and digital issues, fulfilling high-level strategic objectives. According to State officials, elevating the CDP office to a bureau with ambassador-level leadership has enhanced U.S. global engagement and raised the visibility of cyber diplomacy.

For example, in 2024, the Ambassador represented the United States in a trilateral cyber and digital dialogue with Japan and the Philippines, advancing U.S. positions on international cyberspace stability, data security and privacy, and cyber and digital capacity building in Asia. According to State officials, CDP's bureau status also brought senior-level support, increased internal awareness and technical literacy, and allowed cyber policy to take a more prominent role within the department. Officials noted that these organizational changes helped cut through significant bureaucracy, elevated cyber priorities across bureaus, and drew heightened interest in cyber issues.

As shown in figure 1, CDP contains three policy units and a strategic planning unit:

Figure 1: New Entities State Created in 2022 to Elevate Cyber Priorities



Source: GAO based on Department of State documentation (data); Department of State (seal). | GAO-25-108445

- **Office of the Coordinator for Digital Freedom:** supports State's work on privacy, government intervention, human rights, and civic engagement to promote global internet freedom.
- **International Information and Communications Policy:** works to promote competitive and secure networks, including 5G, and to

protect telecommunication services and infrastructure through licensing, sanctions enforcement, and supply chain security.

- **International Cyberspace Security:** leads State's efforts to promote cyberspace stability and security, including diplomatic engagement on international cyberspace security in multilateral, regional, and bilateral forums.
- **Strategy, Programs, and Communications Unit:** responsible for the Bureau's strategic planning, public diplomacy, media, legislative affairs activities, and manages its foreign assistance programs via the Digital Connectivity and Cybersecurity Partnership.

CDP is funded from State's primary operating account, Diplomatic Programs, and annually requests funds from the Diplomatic Policy and Support category, which supports the operational programs of the functional bureaus. In both fiscal years 2023 and 2024, State allocated about \$24 million for CDP to support the bureau and 108 positions. In its fiscal year 2025 budget request, State requested about \$25 million for CDP and to fund two new positions.

In January 2023, after the establishment of the Bureau, State also established the Office of the Special Envoy for Critical and Emerging Technology within the Office of the Secretary (S/TECH) to integrate critical and emerging technologies into U.S. foreign policy and diplomacy. S/Tech leads the development of strategy on the range of priority technologies including AI, quantum, and biotechnology, and coordinates State's internal work on these topics. CDP reports to the Deputy Secretary, and S/TECH reports directly to the Secretary.

CDP Leads Several State Cyber Diplomacy and Foreign Assistance Initiatives

In 2024, we reported that State conducts a range of diplomatic and foreign assistance activities aligned with U.S. cyber objectives.⁸ CDP leads or coordinates several of these activities. For example, State works to build coalitions of countries that share U.S. strategic objectives to (1) counter threats to the U.S. digital ecosystem and (2) reinforce global norms of responsible state behavior. CDP rallies countries that share U.S. goals to coordinate policies that advance an open, free, global, interoperable, reliable and secure internet. These efforts include engaging with the European Union Trade and Technology Council on critical and emerging technologies and with the European Commission to develop

⁸GAO, *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, [GAO-24-105563](#) (Washington, D.C.: Jan. 11, 2024).

shared principles for 6G, a wireless communication network that will succeed 5G.⁹

State officials told us that CDP also facilitates bilateral diplomacy efforts to achieve desired outcomes through activities such as interagency whole-of-government cyber dialogues, which involve communication with partner nations to discuss common interests. According to State officials, such engagement encourages global coordination on a collective strategy to achieve common policy outcomes.

For example, in 2022, State worked with Denmark to advance the Copenhagen Pledge on Tech for Democracy (the Pledge) that counters digital authoritarianism across the globe and advances digital freedom. Following the initial bilateral effort, the Pledge enlisted signatories consisting of civil society organizations, private sector entities, and governments from over 100 countries, advancing goals and values endorsed by the U.S. related to the responsible use of technology.

In addition, CDP works with other agencies through formal interagency agreements and informal processes to leverage expertise and develop a whole-of-government approach to executing key cyber diplomacy activities, including interagency agreements with the Departments of Commerce, Interior, Defense, Homeland Security, the Federal Communications Commission, and the U.S. Agency for International Development. Many of these activities have focused on promoting capacity building, technical assistance, and training for international partners.

Other State Bureaus Lead Cyber-related Initiatives

Other bureaus also lead cyber-related initiatives. For example, State's Bureau of Democracy, Human Rights, and Labor (DRL) established the Freedom Online Coalition (FOC) in 2011, a multilateral forum to build consensus and focus attention on internet freedom. Officials from CDP told us that they collaborate with DRL on relevant issue areas and may provide support by contributing subject matter expertise on specific work. For example, State led negotiations on the adoption of a FOC joint statement condemning Iran's internet shutdowns during widespread protests in fall 2022.

⁹6G is expected to launch in 2030. 6G will have enhanced scalability, greater use of the radio spectrum and dynamic access to different connection types compared to 5G. This will enable greater reliability and reduce drops in connection, which is critical to support advanced technologies such as drones and robots.

In another example, State's Bureau of International Narcotics and Law Enforcement Affairs (INL) leads State's efforts to combat cybercrime. INL led the U.S. interagency effort along with experts in cybercrime policy, technology, and law enforcement from other U.S. agencies to engage with and influence negotiations on a UN cybercrime treaty adopted in 2024.¹⁰ INL also provided technical and other assistance, such as funding for the Council of Europe cybercrime office, which assists developing countries in joining the Budapest Convention on Cybercrime.¹¹

INL contributes funding to the Octopus Project, a Council of Europe cybercrime program established in 2014 to strengthen developing countries' laws to be consistent with the Budapest Cybercrime Convention. This initiative is ongoing and delivers training and technical assistance to developing countries, enabling them to request accession to the Convention. State officials said that providing such foreign assistance helps countries adopt necessary infrastructure protections.

CDP Faced Challenges

In January 2024, we reported that CDP faced organizational challenges that it was still working to address, such as clarifying roles. According to State officials, although responsibilities for cyber issues are defined under the new structure, roles remain deliberately shared and complementary department-wide, making clarification an ongoing challenge.

Officials also noted that because cyber issues may be relevant to almost any aspect of diplomacy, communication within State to ensure awareness and visibility of issues so that expertise is fully utilized is a key, related challenge. For example, DRL and CDP's Digital Freedom Unit cover similar areas, such as free speech on and fair access to the internet. CDP's role is to contribute expertise on tech policy, collaborate with other units to develop complementary positions, and engage with partner countries, whereas DRL advances internet freedom through diplomacy and funding civil society-led projects.

In addition, CDP officials told us that there are some areas of overlap between CDP and S/TECH, such as where AI policy intersects with broader internet governance concerns. They added that CDP's work

¹⁰A/Res/79/243 (Dec. 31, 2024).

¹¹The Budapest Convention is a multilateral treaty that addresses computer related crime. It is global in nature and opened to all countries for signature in 2001. Currently there are 78 parties to the convention. As the Convention is not near universal ratification, State officials told us that any country's decision to accede is significant.

covers overarching cyber and digital topics and partnerships while S/TECH works to leverage international partnerships on emerging technology.

We also reported that CDP was working to clarify State's role in the interagency process and to ensure State maintains the lead in cyber diplomacy and coordinates actions with other U.S. agencies. For example, State in 2023 led a delegation of officials from U.S. Cyber Command, the Office of the National Cyber Director, and the Cybersecurity and Infrastructure Security Agency that met with Ukrainian Deputy Ministers and announced \$37 million in non-military cyber assistance for Ukraine.

Another challenge CDP was working to address was hiring staff. According to State officials, CDP was staffed and operational as of 2023 but needed to train existing staff and hire more people to meet its growth plans. To address existing skills gaps, CDP implemented a knowledge sharing program covering areas such as international cybersecurity partnerships, digital freedom policy work, and interagency coordination. CDP also established a Cyber and Digital Policy Officer course at the Foreign Service Institute and is working to provide it virtually to staff worldwide. CDP's goal was to ensure there is a trained Cyber and Digital Policy Officer at every embassy by the end of 2024.¹²

In addition, as of January 2024, State was establishing a mechanism to identify cyber skills department-wide, added fluency in cyber topics as a selection criterion for ambassadors, and launched an annual "Achievement in Tech Diplomacy" award. To address hiring needs, CDP was implementing and exploring additional hiring mechanisms and developing partnerships with industry, academia, and other agencies to create a talent pipeline. However, the Ambassador told us he recognized that competing with the private sector to hire staff with the right skill sets would be a challenge.

Shortly after we issued our report, State released the *United States International Cyberspace and Digital Policy Strategy* in May 2024. The strategy outlines four action areas to lead the interagency process for coordinating digital diplomacy, ensure consistency in policy and execution, and reinforce State's leadership in international fora. It also

¹²As of March 2025, CDP had trained over 250 cyber/digital officers since 2023, according to a CDP official.

emphasizes the importance of structured engagement with multistakeholder and multilateral bodies to avoid gaps that adversaries could exploit—aligning with CDP’s efforts to engage with other bureaus and external partners through both formal and informal mechanisms. The strategy also identifies specific actions to build cyber and digital capacity among our allies. For example, it outlines plans to strengthen cyber capacity through international partnerships and interagency collaboration.

Our prior work shows that implementing major transformations, such as those outlined in the strategy, can span several years and must be carefully and closely managed. State can look to our leading practices to help assess agency reform efforts to inform its ongoing implementation of the strategy, specifically those related to implementing the reforms and strategically managing the federal workforce.¹³

We have not assessed CDP’s progress toward achieving the goals outlined in the *United States International Cyberspace and Digital Policy Strategy*. Although CDP’s efforts to address its challenges described in our 2024 report appear to support the strategy’s implementation—such as participating in interagency coordination and initiating efforts to build a cyber talent pipeline—it is too early to determine whether these actions are contributing to measurable progress in the strategy’s four action areas. As the bureau continues to mature, additional time and evidence will be necessary to evaluate how effectively CDP is advancing priorities such as building digital capacity, promoting responsible state behavior in cyberspace, and aligning rights-respecting approaches to digital governance with international partners. Further, it will be important to determine how these goals align with the priorities of the new administration.

In conclusion, efforts to promote cyber diplomacy at State have evolved and the formation of CDP has led to higher visibility and prioritization of these efforts. However, challenges remain. According to State officials, clearly defining roles and responsibilities across overlapping issue areas continues to be an ongoing need, particularly given that cyber issues span nearly all aspects of diplomacy. Ensuring sustained internal communication and visibility across State, especially as CDP’s functions intersect with other bureaus, also remains an important challenge. Further, ensuring that the bureau has staff with the sufficient expertise to

¹³GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, [GAO-18-427](#) (Washington, D.C.: June 13, 2018).

carry out its goals is also a challenge, particularly in light of efforts to consolidate State's functions. These are challenges that the bureau will need to effectively navigate if it intends to effectively achieve its mission to lead, coordinate, and elevate U.S. foreign policy on cyberspace and digital technologies.

Chairman Self, Ranking Member Keating, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Latesha Love-Grayer, Director, International Affairs and Trade, at lovegrayerl@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jim Reynolds (Acting Director), Rob Ball (Assistant Director), Benjamin L. Moser (Analyst-in-Charge), Mark Dowling, Thomas Friend, Meg McAloon, Donna Morgan, and Jina Yu. Staff who made key contributions to the reports cited in the testimony are identified in the source products.

Related GAO Products

Products Referenced in This Statement

Cyber Diplomacy: State Has Not Involved Relevant Federal Agencies in the Development of Its Plan to Establish the Cyberspace Security and Emerging Technologies Bureau, [GAO-20-607R](#), (Washington, D.C.: Sept. 22, 2020).

Cyber Diplomacy: State Should Use Data and Evidence to Justify Its Proposal for a New Bureau of Cyberspace Security and Emerging Technologies, [GAO-21-266R](#) (Washington, D.C.: Jan. 28, 2021).

Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities, [GAO-24-105563](#) (Washington, D.C.: Jan. 11, 2024).

Other Related Products

Cybercrime

Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime, [GAO-23-104768](#) (Washington, D.C.: Mar. 1, 2023).

Cybersecurity

High-Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation, [GAO-24-107231](#) (Washington, D.C.: June 13, 2024).

Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy, [GAO-24-106916](#) (Washington, D.C.: Feb. 1, 2024).

Cybersecurity High-Risk Series: Challenges in Establishing a Comprehensive Cybersecurity Strategy and Performing Effective Oversight, [GAO-23-106415](#) (Washington, D.C.: Jan. 19, 2023).

Cybersecurity: State Needs to Expediently Implement Risk Management and Other Key Practices, [GAO-23-107012](#) (Washington, D.C.: Sept. 28, 2023).

IT Workforce

State Department: Additional Actions Needed to Address IT Workforce Challenges, [GAO-22-105932](#) (Washington, D.C.: Jul. 12, 2022).

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Please Print on Recycled Paper.

Mr. SELF. Thank you, Ms. Love-Grayer.
I now recognize Mr. Nemeroff for his opening statement, welcome.

STATEMENT OF THEODORE NEMEROFF

Mr. NEMEROFF. Chairman Self, Ranking Member Keating, distinguished members of the subcommittee, thank you for the opportunity to testify today. My remarks are drawn from my written testimony and offered in my personal capacity.

This subcommittee is reviewing the Cyber Diplomacy Act at a critical time. American leadership and key technologies, especially AI, positions us to shape the global technological ecosystem in ways that align with our values and benefit U.S. national and economic security. But our vision is contested, as my colleagues here has really effectively outlined. China poses the greatest and most comprehensive challenge to U.S. leadership, leveraging both economic and security tools to advance its goals. Russia, Iran and North Korea also pose significant threats and ransomware actors operating with impunity from Russian territory routinely disrupt our businesses, our hospitals and our schools.

Through the Cyber Diplomacy Act. This committee has helped ensure the State Department is better prepared to meet these challenges. A key strength of Congress' vision was to integrate national security, economic and human rights equities in CDP. This has increased efficiency and reduced redundancy within the Department, and unlocked opportunities to face the challenge posed by China in particular in more comprehensive and strategic ways. But we can always do better. I recommend going forward focusing on four areas: First, CDP should take further steps to organize itself around a full-stack approach to cyber and digital diplomacy. Whether our adversaries gain access to critical systems through hacking or by selling untrusted undersea cables data centers or 5G, it all harms our national security, and the Department needs to think about this all together.

A full stack approach enables us to see the full picture and leverage engagements at one layer to have influence at others. For example, the way that our cyber support to Costa Rica, which has been cited several times already, has, since 2022, opened the door to deeper cooperation with the country on telecom issues.

Second, CDP should continue to lead efforts to deter adversaries that behave irresponsibly. Cyber deterrence is not like nuclear deterrence. It requires a dynamic and constant effort, warning adversaries about activities we won't accept and then swiftly, preferably with allies, responding to activities that cross our lines by imposing meaningful consequences.

This effort started in the first Trump administration with coordinated international responses to incidents like Russia's 2017 NotPetya cyber attack, and it continued in the Biden administration with actions like our response to Iran's brazen 2022 cyber attack against Albania, attempting to coerce a NATO ally.

Third, CDP should continue to take on a more operational role, especially in incident response, and by using diplomatic channels to support whole-of-government adversary disruption campaigns. These activities show clear gaps in interagency capabilities that I

saw when I was at NSC working on issues around Ukraine and others.

I want to particularly highlight the potential for CDP's recently piloted falcon capability which allows State to rapidly deploy private sector incident responders to countries in need.

Finally, I want to emphasize the importance of foreign assistance and development finance. We are in a global tech competition with China. We need every tool possible to level the playing field for our companies against China's subsidies and hardball tactics. And a well-placed cyber assistance project, or a well-timed loan can make all the difference. CDP needs funding to provide specialized foreign assistance where it is most needed, and it should be empowered to build a coordinated, full-stack investment strategy across the inter-agency, including with institutions like development finance corporation.

This subcommittee has been—we will be reauthorized in the Cyber Diplomacy Act, alongside the administration's recently announced plans to reorganize the Department.

I offer four key questions to consider as you decide on the way ahead: First, does the proposed restructuring enable the type of integrated approach I have discussed today? Second, does it maintain the requisite attention authority and responsibility of the Department's most senior leaders, the ones who can make this a priority in States regionally oriented work?

Third, does it sustain and ideally accelerate efforts to bill a technology savvy workforce? And fourth, does the proposed budget provide the resources required for this critical mission set?

I want to thank this subcommittee for its continuing leadership and I look forward to your questions.

[The prepared statement of Mr. Nemeroff follows:]

Testimony of Theodore Nemeroff
Co-Founder and Vice President, Verific AI
House Committee on Foreign Affairs, Europe Subcommittee.
Hearing on “Shaping the Future of Diplomacy: Review for State Department
Reauthorization”

April 29, 2025, 2:00 PM

Chairman Self, Ranking Member Keating, distinguished Members of the Europe Subcommittee, thank you for the opportunity to offer testimony on “Shaping the Future of Cyber Diplomacy.” We are meeting at a time when cyber criminals are disrupting our lives and businesses on a daily basis, and nation-states are targeting our critical infrastructure and conducting indiscriminate cyber spying operations. Meanwhile, emerging technologies and the digital economy are among the most powerful drivers of economic competitiveness – a force for change that none of us can ignore. Cyber and digital issues are at the core of strategic competition with adversaries, and central to the future of our democracy and society. If foreign policy is about delivering for our citizens, there is no more important domain in which to deliver.

Opportunities and Challenges

The opportunities for the United States in the coming decade are numerous, but so are the risks. Working with international partners and the private sector, the United States can foster norms of responsible state behavior and a trusted technology ecosystem, reflecting democratic values, that countries around the world will want to adopt. This will reduce the risk of conflict in cyberspace, encourage innovation, and safeguard U.S. national and economic security.

Our affirmative vision will not go unchallenged. China poses the greatest and most comprehensive threat to U.S. technological leadership – whether through its pre-positioning of cyber capabilities on our critical infrastructure and communications systems or its flooding of the global market with low cost but often untrustworthy products across the technology stack – from 5G, to connected vehicles, to AI applications. Alongside Russia, China has taken on an increasingly assertive diplomatic role, seeking to advance their authoritarian vision for the world in venues like the United Nations and technical standards bodies, as well as through hard ball bilateral diplomacy underpinned by economic inducements.

Russia, Iran, and North Korea also pose significant cyber threats. Russia has demonstrated its willingness and ability to carry out disruptive and destabilizing cyber attacks in peacetime, crisis, and armed conflict. And Russian cyber criminals – operating with impunity from Russian territory – routinely conduct ransomware attacks that disrupt governments, businesses, hospitals, and schools in the United States and around the world. Iran, too, has conducted numerous disruptive cyber operations to advance policy goals, including its 2022 cyber attack against Albania, a brazen attempt to coerce a NATO ally. Meanwhile, North Korean cyber actors and IT

workers are generating foreign currency and stealing intellectual property that the regime can use to build weapons of mass destruction and other technologies.

In sum, the United States faces cyber, digital, and technology challenges and opportunities up and down the technology stack, during peacetime, crisis, and conflict. Just as in other domains, diplomacy is a central for advancing American interests in the digital one: deterring adversaries, building partnerships with governments and the private sector, offering technical assistance to victims, safeguarding human rights, reinforcing standards for trusted technology ecosystems, and imposing consequences on bad actors.

Strengthening Cyber and Digital Diplomacy

The House Committee on Foreign Affairs has played an important role in working to ensure the State Department has a corps of cyber and digital diplomats ready to meet the moment. The bipartisan Cyber Diplomacy Act – later codified in the National Defense Authorization Act for 2023 (NDAA) – called for the Department to elevate these issues by creating a dedicated bureau, led by an Ambassador-at-Large. Recognizing the overlap and complementarity between security, economic, and human rights issues when it comes to cyber and digital policy, the NDAA called for the consolidation of the cybersecurity-focused mission of the Office of the Coordinator for Cyber Issues (my former office), with digital economy-focused elements of the Bureau of Economic and Business Affairs, and digital freedom work. The NDAA called for this new organization to – at least initially – report to the Deputy Secretary of State, to ensure this mission set gets the senior level policy attention and focus it deserves and to send a clear signal to our bureaucracy and our partners that cyber and digital diplomacy will be an enduring critical mission area.

Since its establishment in 2022, the resulting Cyberspace and Digital Policy Bureau (CDP) has greatly matured the State Department’s cyber and digital diplomatic capabilities. CDP’s integration of security, economic and human rights expertise increased efficiency across the Department and unlocked opportunities to develop more comprehensive diplomatic strategies that leverage our strengths in all three areas. Through a dedicated program office, with unique cyber and digital expertise, CDP has piloted innovative new foreign assistance projects that advance U.S. interests, for example, by facilitating the connectivity of small island states to U.S. undersea cables and providing critical technical support to partners under major cyber attacks by our adversaries. CDP has also fostered a more tech-savvy diplomatic workforce and strengthened the Department’s capabilities in key policy areas like supply chain security. And CDP has continued to execute core missions, from pursuing strategic cyber stability with our adversaries, to maintaining alliance unity, to advancing the U.S. vision for cyberspace in venues like the International Telecommunications Union and the UN First Committee.

Nonetheless, there is always room to strengthen CDP. As this Subcommittee considers reauthorization of the Cyber Diplomacy Act, I would encourage you to focus on the following key areas, among others:

- **Further advancing a “Full Stack” approach** – CDP should take further steps to develop programs and organize itself in ways that break down the Department’s legacy approach of treating the hardware and software challenges separately – our adversaries certainly do not treat them separately. This should include integrated strategies, working with the private sector, that cut across every element of the technology stack, such as undersea cables, data centers, 5G, AI applications, and the cybersecurity of all of these elements. This is important because every layer of the stack is a potential entry point for our adversaries – it does little good to build a secure undersea cable if our adversaries can access data through a 5G network they built or simply by hacking into a data center or telecom network, as we say in Salt Typhoon. In my experience, working with a country on one layer of the stack provides opportunities to shape their approaches at other layers, but if only we are intentionally approaching our engagements in a full stack way. This was certainly the case in Costa Rica, where critical and timely cybersecurity assistance that we provided at a moment of crisis helped open the door to deeper cooperation on trusted telecom issues. Similarly, U.S. international messaging around threats posed by Chinese connected vehicles became more credible and convincing to other auto-producing countries when we discussed them alongside efforts to secure all connected vehicles from cyber threats.
- **Deterring and punishing adversaries that behave irresponsibly**– Across multiple Administrations, the Department has helped pioneer the U.S. government’s approach to deterring adversary cyber activities. CDP should continue its work as a leader on cyber deterrence, innovating on new ways to work with partners in the Indo-Pacific region to deal with threats from China and to build on coalitions like the Counter Ransomware Initiative to change the incentive structure for criminal actors. Clear messaging to our adversaries about the activities we will not tolerate, clear cooperation and solidarity with allies and partners to support victims and build a response, and clear consequences – whether sanctions, asset seizures, visa bans, or Rewards for Justice bounty offers that target and isolate individual hackers – for actors that engage in disruptive and destabilizing behavior is essential to making our adversaries think twice about launching disruptive operations. These efforts should be underpinned by consensus norms of state behavior that the United States has championed for over a decade. While our adversaries routinely flout cyber norms, particularly with respect to countries that are weaker than them, they provide a common ground to build coalitions with other countries against our adversaries’ bad behavior. State should be encouraged to explicitly call out norm

violations when we see them and get other countries to join us in imposing consequences, like complementary sanctions or asset seizures under their own authorities.

- **Strengthening incident response and adversary disruption capabilities-** Since CDP's establishment, the Department has taken on an increasingly operational role in dealing with cyber threats that fills gaps and complements the work other cyber-focused Departments and Agencies. This was something that I saw a significant need for when I was on the National Security Council staff during incidents like the Iranian cyber attack on Albania. One thing that I particularly think we need is an international incident response capability that complements investigative and other U.S. and victim government efforts on the ground. CDP's recently piloted Foreign Assistance Leveraged for Cybersecurity Operational Needs (FALCON) capability allows it to deploy teams to help partners remediate international incidents on short notice. Such deployments, in circumstances where other U.S. agencies do not have appropriate authorities or resources, position the U.S. government to safeguard our interests in cyber-related crises and can generate valuable insights for domestic cyber defense. In addition, the Department plays an important role in using information sharing through diplomatic channels and capacity building, in concert with cyber and law enforcement-focused agencies, to help other countries disrupt adversary cyber operations targeting them. These diplomatic campaigns, which often accompany major public releases of Chinese or Russian cyber threat indicators by U.S. cyber agencies, are a great way to build partnerships with other countries, while complicating adversary cyber operations in a way that makes us safer at home. Both of these operational lines of effort have a multiplier effect on interagency cybersecurity work.
- **Coordinating foreign assistance and development finance-** At a time when the Administration is reassessing its foreign assistance priorities and funding levels, this Subcommittee should recognize the strategic importance of putting U.S. government resources behind building a trusted global technology ecosystem, underpinned by U.S. cybersecurity knowhow. This is a critical time. The digital infrastructure being built now will have a huge impact on AI and other applications rolled out tomorrow. If Chinese companies – using the uneven playing field created by government subsidies – are able to dominate the build out of digital infrastructure in developing countries and layer on top of this infrastructure open-source models like DeepSeek's R1, the Chinese will gain significant economic and political leverage. We need to make sure that our companies can make competitive offers. A well-placed cybersecurity or digitally focused foreign assistance project or a well-timed loan from the Development Finance Corporation (DFC) can make all the difference in leveling the playing field for our companies and private investment in countries that still deeply respect U.S. technology leadership. But to do this, CDP should be empowered. It should be given sufficient foreign assistance

resources that it can direct strategically. CDP also should be given a clear mandate to build a coordinated and country-specific-investment strategy across the interagency, including with entities like the DFC. We should also continue to leverage foreign assistance to foster effective cyber and technology regulations in rapidly digitizing developing countries to enable private sector investment and avoid the pitfalls of both our adversaries' authoritarian models and some of our allies' over-regulation.

Organizing Cyber and Digital Diplomacy in the State Department

This Subcommittee will be reviewing reauthorization of the Cyber Diplomacy Act in the context of the Administration's recently announced plans to reorganize the Department. State Department modernization is an important and challenging task. As the Subcommittee considers the way ahead, I encourage you to be guided by a few key criteria:

- **First, does the proposed restructuring enable an integrated approach?** This should not be a question of “balancing” security, economic, and human rights interests across different siloes in the Department, but leveraging strengths in each of these spheres to advance American interests.
- **Second, does it maintain the requisite attention, authority, and responsibility of the Department's most senior officials?** This is the only way to ensure the Department's regionally oriented work gives emerging issues the focus they deserve. It also will position the Department's leadership to advance our technology agenda in each and every one of their diplomatic engagements, whether it is promoting American business, reviewing cyber operations, safeguarding our supply chain, or calling out human rights violators.
- **Third, does it sustain and ideally accelerate efforts to build a technology-savvy diplomatic workforce?** Reform is not just about moving boxes on the org chart – it is about creating the right incentives and mechanisms to prioritize hiring, training, retaining and promoting people with technology-focused talent, not only in CDP but across the Department.
- **Finally, if budgets reflect priorities, does the proposed budget provide the resources required for this critical mission set?** The budget needs to provide sufficient operational resources so that we can deploy our cyber and digital experts where they are needed around the world. And our diplomats need to continue to have assistance resources – CDP spent \$115 million in FY23 foreign assistance funds and was projected to spend \$140 million in FY24 – so that they can pair their talking points with concrete offers of support.

Concluding Thoughts

I want to thank this Subcommittee for its continuing leadership to ensure that cyber, digital and technology diplomacy remains a priority for the Department. As we compete with adversaries and seek to advance an affirmative U.S. vision for the technology landscape, there is no more important area for our diplomats to excel. I look forward to answering your questions.

Mr. SELF. Thank you, Mr. Nemeroff.

I now recognize myself for 5 minutes of questioning. A series of questions, Ms. Fixler. You say Taiwan survived the attack. What did you mean when you say, survived the attack? Is that physical or is that cyber? What are you referring to?

Ms. FIXLER. Sure so in the tabletop exercise we did, it was a series of economic and cyber attacks that were testing the societal resilience of Taiwan to withstand Chinese aggression and withstand efforts to coerce its policy to agree to a reunification with the mainland, so it was a societal and cyber resilience. And if the CPP judged that Taiwan could survive the pressure campaign, it might actually—

Mr. SELF. By not go kinetic.

Ms. FIXLER. Yes.

Mr. SELF. Okay. I want to read something to you. Yesterday, probably everyone in this room was aware of the three-nation outage in Europe. I got back from Europe a week ago Saturday, so this is from the Siemens Security Advisory, just to show you how important this issue is, the point of origin for the blackout possibly originated—when they say possibly, they are not definitively saying something, but I believe that they believe this, possibly originated in a high-voltage substation in the Basque region of northern Spain specifically near Balboa at the substation that they named. The potential method of sabotage was a sophisticated cyber attack targeting the substation SCADA system, injecting malware that overloaded transformers and triggered a cascading failure across the European grid. The malware exploited a known vulnerability in the Siemens system and they listed that.

So Ms. Fixler, you, in your testimony you mentioned the need for partners and allies to be cyber resilient. When I was in Europe, I talked to both politicals in Europe and to our U.S. military, and they made the U.S. military from the SAC (ph) on down said that we need to be aware that their infrastructure to include cyber needs to support our war plans. Can you elaborate on what you said about their vulnerable infrastructure impacts our national security?

Ms. FIXLER. Sure, thank you so much for the question. So we recently at FDD issued a report looking at military mobility, specifically the way that U.S. military forces rely on civilian critical infrastructure to move men and material in the United States. That is true as well overseas, and we intend to look more closely at the infrastructure in our NATO allies and how it must be secure so that our troops have secure transportation infrastructure, telecommunications infrastructure, because all of our forces rely not on infrastructure-owned and operated exclusively by the Defense Department, but by civilian-owned infrastructure. So that infrastructure must be resilient to secure our forces overseas.

Mr. SELF. Thank you. Ms. Love-Grayer, in what way has the CDP worked with other agencies to advance cyber diplomacy? How does that impact national interest, defense interest? And where is the coordination point? And who holds the big stick, I will call it, in this area, cyber diplomacy?

MS. LOVE-GRAYER. Thank you for that question. I actually have several examples. But I want to use one that connects to what you

just mentioned. So the DOD has an operation called Hunt Forward, where they assist our partner countries by assessing their vulnerabilities in their cyber systems. CDP partners with them by going in afterward and actually providing the technical assistance and capacity building needed to address the vulnerability that they have identified. And so again, if we are partners with those countries and we are working with them closely, we may even have our own troops in those countries. It is important to not only identify the vulnerabilities, but to help them to address it.

In terms of the coordination, there are various ways that CDP coordinates that we found in our audit. There is informal regular meetings between the heads of corporations and the agencies and with private sector corporations. But also, there is formal inter-agency agreements. So CDP at the time that we conducted our audit had 11 different agreements with different agencies such as DOD, Department of Commerce, the FCC, DHS, USAID and others. And these interagency agreements allowed them to partner with these other agencies who have specific capabilities and skill sets that could be used to provide, again, technical assistance and capacity building to other countries.

Who has the big stick? At the moment, it depends on—I would say, depending on what you call the big stick. I think who has the mandate for cyber diplomacy is CDP. Sometimes it is the other agencies who might have the technical expertise or even the funding. CDP does provide foreign-assistance funding, but in other cases they may just partner. So CDP has the mandate and there are a number of other players who have different types of capabilities that they bring to the table.

Mr. SELF. Very good. I now recognize Ranking Member Keating for 5 minutes.

Mr. KEATING. Thank you, Mr. Chairman.

I think when we use terms like cyber diplomacy and other terms like that, it really doesn't give us back to the real threat that we have. It sounds something that wouldn't be like a direct kinetic attack or something that we had.

But cyber, unlike other kinds of warfare, or other kinds of threats, there is no barriers there, there is no wall that can be built, there is no ocean that stands between these threats. They are global and they have to be approached globally. And so, we really rely had on our allies in this area even more in some respects than we would through conventional kinds of threats that we deal with. So how important is it to have us make sure we are working in these areas, making sure we are funding the cuts to USAID and the other things that could have an effect on our ability to work with our allies? Because if we are working America alone will just not work when it comes to cyber. So how great a threat is that and what should we be looking for? Mr. Nemeroff.

Mr. NEMEROFF. Thank you. I think it is a long old saying that cybersecurity is a team sport, both within the interagency and with our allies and partners. The key thing is to be able to work with allies and partners at different levels of cyber capacity and cyber capability. So in NATO, for example, we work across the board to try to raise the level of cyber hygiene and cyber capability. And then with particular countries, particularly those that are foreign-

assistance eligible, foreign assistance is a fantastic lever to be able to help them help themselves. I think that is the key piece of this. Albania is a NATO ally. Albania was targeted by Iran by a major cyber attack that I think really implicated alliance-wide issues, and having foreign assistance as a way to get them to raise their capability was an important way of achieving our policy goals and to make the alliance safer.

Mr. KEATING. I think readiness is a really clear comparative here too, because timing is so important. Ms. Fixler, you mentioned how quickly the response has to be, and that is critical to being able to deal with this. And it has to be in place ahead of time.

So another question I have, in our own internal domestic workforces there to support this, I am concerned with a lot of these cuts that are going on and the effects on the workforce and the expertise that could be walking out the door here, how important is it to have a workforce that is already trained, experienced, in place? And what would happen through reorganization or cuts, that that was reduced and we lost that? How much of a threat would that create?

Ms. FIXLER. I would just say that thank you for the question. Recruiting and retaining technical talent is a persistent problem in the Federal Government across the Federal Government. At least part of it is a pipeline problem. We need a lot more STEM graduates. We need a lot more folks focused and pursuing cybersecurity degrees. Not all of them need to be 4-year degrees, associates degrees are great, on-the-job training is great, apprenticeships are great. And so I am particularly heartened by some of the efforts in this Congress to focus on cyber workforce, including things like the PIVOT Act providing a faster way for community college graduates to get into the Federal Government with cyber degrees, because we need a lot of cyber professionals in our government to focus on cybersecurity and the intersection between cybersecurity and national security.

Ms. LOVE-GRAY. I will just add a few thoughts to this. One of the concerns that we had after we conducted our review on CDP is that they did need to recruit a specific type of official. They needed someone who had not just technical capability, but also diplomacy skills. And competing for that, as we spoke with the former Ambassador of CDP, he noted it is very hard to compete with the private sector for individuals who can harness both of those skill sets. And so having the staff is once you get them on board keeping them and helping them to grow and understand the issues is important, but also having staff who can really cover the range. There is a broad spectrum of issues involved in cyber diplomacy.

Mr. KEATING. Yes, with 30 seconds left too, Mr. Nemeroff mentioned AI, and this is just going to accentuate and geometrically affect our ability to respond in any timely fashion. And one of my concerns is with the reorganization, there could be siloing of different functions. And the whole point is to bring it all together and perhaps any kind of written responses that you might have, since my time is running out, you could really comment in greater detail on the threat of that siloing and how—we should be looking at reorganizations so that there is not greater difficulty in being able to respond to these really critical threats. I yield back.

Mr. SELF. I now recognize Mr. Davidson for 5 minutes.

Mr. DAVIDSON. Thank you, Chairman. Thanks to our witnesses for your testimony and your preparation for this hearing.

Ms. Fixler, you argued in a March 17 op-ed that cuts to USAID harm our cyber assistance to allies and partners. I mean, by definition, if we don't give them money, we are harming the assistance, but are they really harmed? And I guess to what extent do we want to preserve it? I think you make the case that this could and should be consolidated under CDP. What is the appropriate amount and kind of cyber assistance that the United States should be distributing?

Ms. FIXLER. Sure, thank you for the question. So I think one of the things that CDP has demonstrated it is good at is using a little bit of U.S. foreign assistance, marrying that with assistance from U.S. partners and allies and private sector investment. So I will talk about the undersea cables area because that I think is where this shines. U.S. technology companies, communications companies are making major investments in undersea cables. They are interested in connecting major population centers because that makes sense from a market perspective.

When CDP is able to get involved, it can use a little bit of foreign assistance, find U.S. partners and allies who are interested in the issue, and then combine that with the private sector investment so that we look at it from a strategic perspective. And we don't just focus on the market, but also on where it matters for U.S. military capabilities, particularly in the south—the Indo-Pacific, but that is applicable in other areas as well.

Mr. DAVIDSON. Yes, thank you for a very concrete illustration. And as you talk about blending public sector work to try to foster some private sector investment, one of the big things that we are trying to do as a Congress, really as a country, but we need a law that my other subcommittee might as chairman of the national security, I went to finance, we are working on outbound investment. So I wonder, Mr. Nemeroff, as you think about AI, in particular, one of the most rapidly changing tech sectors and you think about cyber and other factors, what kinds of things ought we to consider within cybersecurity? I think the real tension comes between one approach that says, we don't want American companies investing in AI outside of America, or maybe a more concrete example that uses kind of the financial services' Treasury thing and saying, Here is specifically who we don't want you investing with. What are the tradeoffs there and what is your view?

Mr. NEMEROFF. Thank you. So there was a hot AI competition happening right now among companies and among countries. And we have to think very strategically about that. Cybersecurity comes into it in a lot of different places, but critically in this area in protecting the hard one IP that our companies produce in developing AI models. And so, I think it is important to be thoughtful when one is building data centers anywhere, whether it is here in the United States or elsewhere, how do we build in the right cybersecurity systems in order to protect—and protect our assets from others who might try to steal them for advantage?

Mr. DAVIDSON. Yes, nation states that might use their intelligence services to steal American intellectual property.

Mr. NEMEROFF. Absolutely.

Mr. DAVIDSON. Like China?

Mr. NEMEROFF. Like China.

Mr. DAVIDSON. All right. So that is exactly what we are trying to cutoff. And of course they don't say, Hey, we are with the Chinese intelligence service, they set up companies and they use it to steal it. That is why we really want to go with a sanctioned-oriented approach. I think where you go named individuals and named companies that basically you create a burn list and which keep it going.

So we will see where that goes but hopefully, we will get that done.

You know, one of the tradeoffs there is always civil liberties, so we find people that say, You know, we are really concerned about freedom of speech, Congress, of course, isn't. According to the First Amendment supposed to make any laws abridging the freedom of speech. What can our committee do by working with CDP, because that was the claim that they were just combating misinformation and disinformation. When CISA was frankly it seemed pretty Orwellian, I mean a lot of my constituents had a lot of concerns about an American Big Government agency saying what an American citizen is saying is somehow foreign misinformation. How do we get that right?

Mr. NEMEROFF. Fundamentally, the First Amendment kind of has to be at the bedrock of everything that we do. We do have a challenge that adversaries seek to use the openness of our system to exploit and disrupt or cause—to advance their agenda, that has got to be a part of the consideration. CDP's focus primarily has been on promoting freedom of expression and digital freedom abroad, and in particular, safeguarding our networks and other people's networks from cyber threats.

Mr. DAVIDSON. I think that is the proper focus. I think CISA definitely got it wrong and frankly some of these agencies that were created to defend America were weaponized against American citizens. We want to make sure that we prevent that from happening. Maybe the best way to do that is to hold some of those former officials accountable.

Thanks. My time has expired. I yield back.

Mr. SELF. I now recognize Representative Amo, Mr. Amo?

Mr. AMO. Thank you, Chairman Self. And thank you to our witnesses for being here. Look, it is no secret that digital technologies are quickly evolving, brain—greater connectivity and new and emerging threats. And these threats are not unique to the United States. They transcend borders and affect their allies from across the world. They require close collaboration and global solutions. And starting under the first Trump administration there was bipartisan consensus that America needed a crosscutting bureau, reporting directly to senior State Department leadership that could coordinate the various elements of cyberspace, digital technologies and global digital governance.

The Bureau of Cyberspace and Digital Policy, and I know we are all associated with the acronym CDP now was born in 2022. And its mission, I think, is one to come back to, to underscore, to ensure an open, secure, and reliable internet, a necessity to promote demo-

cratic values like privacy, freedom of expression, access through information.

CDP made our foreign cyber policy more efficient and streamline our cyber diplomacy. But Secretary Rubio's new reorganization plan for the State Department breaks CDP. And I think it is important to highlight these changes. It is separating its economic functions and moving cybersecurity into the new emerging threats branch. This plan undermines the core reason CDP was created, again streamlining international cyber policy.

It is not efficient to create overlapping and redundant mandates. It is not efficient to jeopardize how CDP coordinates cyber policy with the Department of Defense, Homeland Security and the intelligence community. And it is not efficient to jeopardize the essential work that CDP does, alongside the cybersecurity and infrastructure security agency or CISA, because we know that CDP manages programs for CISA that provides training and resources to protect targeted countries from cyber attacks. And given that CISA already faces drastic cuts to their programs, thanks to the actions of President Trump and Elon Musk, ending coordination with CDP could cause tremendous harm in keeping Americans safe.

So Ms. Love-Grayer, how does CDP coordinate with CISA to ensure that we have a comprehensive strategy for cyber diplomacy? And how would the plan on the table from Secretary Rubio split up—splits up CDP, affect their collaboration with agencies like CISA?

Ms. LOVE-GRAYER. In the past we found that CDP, and in particular, the Ambassador-at-large who led it, coordinated very closely with CISA, with the Office of the National Cyber Director to ensure that our domestic policy and our foreign policy, our foreign facing policy aligned so that our views, our perspectives, our policy interests, and our values would be represented in the foreign policy that we had as we faced and engaged with our multilateral organizations. So there was a lot of coordination there.

At the same time, the views and the interests and the issues that the Ambassador heard out in the world, he would bring back to our leaders here on the domestic side to ensure that we could learn from that as well, that we were using that to inform our strategies and our own protections at home. So that collaboration we found to be pretty important.

In terms of where they sat, it was very important that the Ambassador did report to the deputy secretary because he had more direct influence and the ability to get leadership support on major decisions. That coordination sat above all the other bureaus, and so there was a higher level of gravitas that was given to CDP in being able to garner resources and support across the Department is what we found. So breaking that up could look different in the future.

Mr. AMO. And no better time to elevate and make sure that gravitas of that coordination is central while the threats grow by the day.

Before I wrap up here, last week back at home in Rhode Island, I joined Rhode Island College to recognize their designation as a National Security Agency center of academic excellence. And during that time we spent together, we discussed the need for a well-

trained and stable cybersecurity workforce and a pipeline. And one of the things that I certainly would welcome your responses in writing as my time wraps up, we have seen this disdain from a President for public service and Federal workers and firing employees. And so, I want to ask a different version of what the ranking member asked previously just to assess the firing and how it has—of workers and how it has affected our future ability to attract. And I know that might require you to speculate a little bit, but clearly, there is an impact, a lasting impact that in the termination of employees, you know, for no reason will have on the cybersecurity workforce. It will make us less safe. And I welcome your thoughts on that in the future. With that, I yield back.

Mr. SELF. Thank you. Before I introduce our next speaker, the ranking member has asked for a comment.

Mr. KEATING. Thank you, Mr. Chairman.

As you are aware, since our last hearing, we had a discussion, and you expressed that you intend to continue a manner of introduction of a member that at a minimum, is not becoming of this committee. I hope you reconsider. I want to make clear my objection to the harmful, wrong-minded language of the chairman's introduction. It is the wrong way to treat duly elected Members of Congress. It is the wrong way to treat a colleague. The wrong way to treat any individual. The chairman knows, I suggested to both maintain dignity and respect the committee, while continuing our committee's focus on policy issues, that the chairman simply address members by their title if he wants, Representative. But the chairman has said to me that he can't do that because it is just not him.

Representative McBride, on the other hand, has publicly indicated this had he wants to focus on committee policy at hand. Representative McBride has identified who she is, the chairman has identified who he is. And I think it is something to reflect on each time her introduction is disrespectfully invoked.

I yield back.

Mr. SELF. With that, in order—I find myself in the position in order to maintain the parliamentary integrity of this hearing with being the lone majority member here, I would like to recognize Representative McBride.

Ms. MCBRIDE. Thank you, Mr. Chairman. I appreciate that, thank you. That means a lot. And thank you, Ranking Member Keating, for your friendship and your support. Thank you so much to our witnesses for joining us today for your perseverance through a hearing.

Cyber diplomacy has never been more important to American national security interests, and it will continue to grow in its significance in the years to come. This is why the administration's proposal to reorganize the Bureau of Cyberspace and Digital Policy deserves serious consideration and security. And today, we should be asking ourselves does the proposal by the administration make America safer, stronger and more prosperous?

Unfortunately, in just 100 days, the Trump administration has attempted to undertake massive and disruptive changes in how our Nation conducts our diplomacy, throwing our entire national diplomatic ecosystem into upheaval. While serious and thoughtful re-

forms on how the U.S. can best defend our interests abroad should always be welcome, far too many of this administration's actions have been rushed, misinformed and often downright incoherent.

America's diplomatic and soft power is one of our most valuable assets. And Congress' role is to ensure our foreign policy continues to align with our national interests. I promised I would work with anyone who is willing to work with me to deliver for Delawareans so I am looking forward to learning more about this administration's plans.

My first question is for you, Mr. Nemeroff. As emerging technologies transform global digital infrastructure, how can CDP stay ahead of the curve? And what resources or capabilities do you think CDP needs to stay competitive?

Mr. NEMEROFF. Thank you for the question. I am going to come back to the idea of looking at this from a full-stack approach. This isn't a matter of us competing with one technology, but thinking about how we are working to promote a trusted technology ecosystem around the world. Undersea cables, older technology like undersea cables and data centers, and then 5G networks, that is going to shape a lot of what then gets rolled out in terms of AI in different countries as well.

We have stiff competition from models like DeepSeek that are open source and low cost. And so a key piece, in my view of what our strategy needs to be, is thinking about how are we building that entire stack to enable our technology to get out there. And then how were we using cybersecurity? In our remarkable capabilities as a government and a society and our private sector to secure all of those pieces so that we can trust that our information and our ideas can be used safely and without causing harm to our national security.

Ms. MCBRIDE. Thank you. Ms. Love-Grayer, how does the Trump administration shuttering of U.S. foreign assistance writ large impact the ability of the CDP bureau to effectively conduct outreach to allies and partners? What impact do you think the cessation of cyber-related foreign assistance has on CDP's ability to carry out its mission?

Ms. LOVE-GRAYER. We haven't yet assessed the effects of these changes, especially since they are not formalized. But I will say we do have a request, a congressional request to look at the impact of foreign assistance changes, including to the workforce and so we plan to do that soon.

Ms. MCBRIDE. Thank you very much.

I want to reiterate the comments of my colleague, Representative Amo and the ranking member made earlier about the importance for us to provide a respectful, predictable, sustainable career option for public servants across the Federal Government. And this is an area that obviously requires specific training, specific skills, which makes it that much more difficult to recruit for and retain in, especially when competing with the private sector. And I think it is important as we have these conversations to recognize the importance of protecting our Federal workforce and treating them with respect as we seek to fill these positions and have the best and brightest working in this critical capacity so thank you very much.

Mr. Chairman, I yield back.

Mr. SELF. Thank you, I recognize myself for 5 minutes.

We are leading on this CDP reauthorization. I have several questions, for everyone's information here, we have nongovernmental witnesses here because we don't have a lot of people confirmed yet. So that is why we have you. And I appreciate you all filling in the gaps while we can.

So a couple of—first of all, for you, Ms. Fixler, undersea cable routing, because we have seen undersea cables being torn up in several different theaters of the world. Is this an area that we ought to be engaging with our allies? Because—is there any way to protect the undersea cables or route them which would help national security?

Ms. FIXLER. Sure. Thank you for the question. Undersea cables are a critical issue. And it is both the physical resilience and the cyber resilience of that infrastructure. And the ownership and operation of that infrastructure.

China and Russia have demonstrated they are interested in disrupting that infrastructure. And China has also demonstrated that it is interested in owning operating that infrastructure so that it can route and control the flow of communications. And so, it is concerning when our adversaries are trying to disrupt the infrastructure, and when they are trying to control the infrastructure.

Mr. SELF. Okay, thank you.

I just want to get to the specifics here. We are talking about cybersecurity professionals. Give me a range of—first of all, what level to we need in the CDP and what would be a range of salaries? Who wants to tackle that? Ms. Love-Grayer?

Ms. LOVE-GRAYER. Well, I think I will tackle part of this question. We are talking about cybersecurity, but also beyond cybersecurity, there are a range of cyber issues and technical capacities that are needed, and you need diplomacy skills as well. One of the things we heard from CDP after our review is that they had trained about 250 diplomats on cyber issues. So there is internal training you can do, as well as hiring, and I think we need to use both capabilities.

Mr. SELF. So what about salary range? Who wants to tackle that? Because we are competing with a growth industry here.

Mr. NEMEROFF. I can start. The one piece I would emphasize, I am a lawyer by training—

Mr. SELF. I am sorry.

Mr. NEMEROFF. Yes. And I think what I learned in legal cyber practice has also been true in diplomatic cyber practice, which is that you take the old skills and you apply it to a new technology. And so that is a lot of what CDP does really well, it brings in diplomatic whizzes who can learn the technology and apply it. And it brings in tech whizzes who can learn the diplomacy and do that too.

Salary is a problem, we operate on the normal GS-15 scale so there is no special cyber pay at the State Department, and I do think that is an issue that you have colleagues who can—

Mr. SELF. No, I am asking, what are we competing against?

Mr. NEMEROFF. In the private sector?

Mr. SELF. Right.

Mr. NEMEROFF. Hundreds of thousands of dollars.

Mr. SELF. Okay. I do want to get to because several mentions have been made of the new org chart. I want to just hear briefly—I have less than 2 minutes here. Let's go down the line, what do you recommend? I think part of it was in your written testimoneys, part of it was in your verbal testimoneys, but I want to hear specifically what do you recommend for CDP in the reauthorization, quickly.

Ms. FIXLER. I will jump in. I think Congress had it right on a bipartisan basis, you created the cyber bureau and you understood the importance of the integration between the different components of the cyber mission, the cybersecurity mission, the digital economy mission, the emerging threats mission. All of those work hand in hand. And so, seeing that integration remain I think is a wise decision Congress previously made. I look forward to Congress continuing to weigh in on that.

Mr. SELF. But now, it is directly underneath the deputy secretary. It is probably not going to stay under the deputy secretary.

Ms. FIXLER. Yes, or maybe. I mean, you are going to reauthorize right it. Thank you for the question, though. I think the integration of the bureau is where I would focus. Whether—the head of the bureau needs to have the authority in crosscutting authorities, but whether exactly where you position the bureau I think may be less important than the integration of the different capabilities within the bureau.

Mr. SELF. Thank you.

Ms. LOVE-GRAYER. Actually I really agree with this point. I think integration is really critical even as we interface with other governments who are structured differently. However, I do think that where it sits plays an important role as well, because depending on where it sits it may have to compete with others for resources. And it also needs the ability to have the leader communicate with the most senior leaders at State in order make some pretty important decisions.

I would consider where it is placed. It also says something about what where the focus is. If it is in the E bureau versus the T bureau, it sends a signal about what the focus of the bureau will be, or the E family versus the T family.

Mr. SELF. Out of time. But quickly, Mr. Nemeroff, I very much agree with the point about maintaining integration. There is no perfect answer, if you are going to try to put it under E or T, I think you need to make sure that whoever it is reporting to cares about the whole mission and that senior leaders at the top of the department the deputy secretary are still going to be representing all the equities that deputies committee meetings and diplomatic engagement.

Mr. SELF. Thank you, I recognize our ranking member.

Mr. KEATING. Ms. Fixer mentioned the tabletop exercise that occurred. I am just curious as part of that, since I am also in the Armed Services Committee, we are boosting our undersea autonomous vehicles, and we have been doing it every year because of threats like this.

Did you—is any of that considered, I know it is not strictly cyber, but we have been talking about the integrity of undersea cables?

Ms. FIXLER. Yes. Thank you for the question. I am happy to provide more information about the exercise that we conducted. We have an after-action report, I am happy to share that with the committee.

The exercise looked at a number of different attacks that China could conduct. Some of them were cyber-related. Some of them were sort of more in the economic realm. And they looked also at undersea cables, mostly the disruption and the need to be able to quickly repair that infrastructure.

Mr. KEATING. The other thing is, I remember my time in homeland security, how we were trying to deal with cyber threats and the importance of dealing with the private sector, because many of the countries that are represented, as well as our own, that is done on the private side and has an enormous impact to our safety and economy.

The same is true for the other countries that we are trying to make more resilient and make sure we are not affected by things that affect them.

So when you are looking at that situation and you are dealing with a private side, can you explain advantages there might be with the fact that we can deal with other countries to deal with their own private sector instances in terms of getting that kind of cooperation, particularly in revealing a cyber attack, you know, just minutes, hours make a difference in the ability to contain that. Perhaps anyone might want to address that.

Mr. NEMEROFF. It was particularly breathtaking, I thought, to see the scale and speed and agility of the private sector in the days after the Russian invasion of Ukraine. They were able to move at a speed I wish governments could move at, and so, they are a critical partner wherever you are operating.

I found that foreign assistance is a part of it, but another part of it is maintaining a shared situational awareness.

The reporting that you referred to that they often issue is really an early warning often of incidents that we need to respond to quickly, and so they are a critical partner.

Mr. KEATING. Great. Thank you. I notice we have another member who has come for a first line of questioning, so I yield back.

Mr. SELF. I now recognize Mrs. Kim.

Mrs. KIM. Thank you, Chairman Self. Thank you. I want to thank our witnesses for being here today. You know, let me go right into questions like, how can private sectors' technological expertise such as that from organizations like very fake AI be leveraged to enhance the resilience of ally infrastructure against the response of a cyber attack?

Mr. NEMEROFF. Thank you. I think it is a critical thing that every country in government needs to recognize that this has to be a public-private partnership, and that governments need to rely and use private sector capabilities to secure their networks.

We have made important strides within the U.S. Government, for example, moving to cloud as a place to store our data in order to help take cybersecurity out of the hands of individual offices and place it higher up.

We have also found that when incidents happen, private sectors are often the most agile in investigating and remediating, and so,

it is very important as we talk to our allies and partners to make sure that they are thinking about this as a team sport as, well working with their own companies, or working with capable U.S. cybersecurity providers in order to provide these kinds of services and support.

Ms. FIXLER. I would just add as well, CDP maintains some of those relationships, and its incident response capability, the foreign assistance funding that you all authorized to focus on rapid response and rapid deployment of resources, that is a partnership with private sector companies. It is not deploying U.S. Government personnel, but it is the relationship with private sector cybersecurity incident response professionals.

Ms. LOVE-GRAYER. I will add just one note, which is, CDP's foreign assistance also sometimes makes it capable—or makes the environment possible for private sector companies to come in. And we saw that with Costa Rica, because they changed their environment based on CDP assistance, Intel felt more secure in being able to go in and make a \$1.2 billion investment that they probably would not have made if Costa Rica had not changed many of its cyber norms and policies as a result of its interactions and engagement with CDP.

Ms. KIM. Thank you. You know, Ms. Fixler, from your perspective, how should the CDP bureau foster such partnerships to enhance cybersecurity in ally infrastructure, and what challenges must be addressed to ensure effective cooperation across the borders?

Ms. FIXLER. Thank you for the question. I will focus specifically on the challenge. I think there is a challenge to think about things strategically. When it comes to critical infrastructure, everything is critical, but, frankly, there are things that are more critical, and we need to focus on that systemically important infrastructure in our own country and abroad to think about what do we most need to protect against. So if we can think about that strategically, I think that is a challenge, but a real opportunity for us to do better.

Mrs. KIM. Ms. Love-Grayer, can you provide which offices GAO found to have overlapped with CDP, and how the bureau works to ensure clear delineation between responsibilities with other offices that have cyber equities?

Ms. LOVE-GRAYER. Within State, we found that the Bureau of Democracy and Human Rights and Labor, DRL, as well as INL, which focuses on international law enforcement, both of those bureaus also have equities in cyber diplomacy.

DRL, in particular, works on freedom, internet freedom issues, and they engage in multilateral foreign—they provide foreign assistance.

INL works on combating cyber crime. And they also lead a lot of the foreign assistance initiatives with other foreign governments, as well as multilateral diplomacy efforts.

So the coordination between all three of them are important. We found that they do have regular meetings and conversations, but they were still facing challenges defining who should take the lead on certain initiatives given the expertise that already exists in these other bureaus.

Mrs. KIM. Let's talk about that, so can you talk about the steps that CDP can take to mitigate risk of the overlap or redundancy that you are talking about in existing cybersecurity efforts across the Federal agencies, and how has CDP improved collaboration with key partners like DHS, DOJ, DOD and Treasury?

Ms. LOVE-GRAY. Within the Department, one of the things they—I believe they have started to do and they can continue to do is ensure that there is constant communication between all of the bureaus and they are well aware of which partners they are working with and where the focus ought to be for each one of them.

There is still some overlap in the missions, and I think there could be greater delineation between who is taking the lead on certain issues if they are not going to be consolidated in any kind of way.

In terms of the interagency, currently they have formal inter-agency agreements with several agencies, DHS, DOD, FTC, Department of Commerce, those do seem to be working well because they outline the parameters of those relationships and who is taking the lead.

Mrs. KIM. Thank you. Chairman, I yield back.

Mr. SELF. I thank the witnesses for their testimony, and the members for their questions. The members of the subcommittee may have some additional questions for you, and we would ask you to respond to those in writing.

Pursuant to committee rules, all members may have 5 days to submit statements, questions and extraneous materials for the record subject to the length of limitations. Without objection, the committee stands adjourned. Thank you very much.

[Whereupon, at 3:27 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD



Chairman Brian Mast

**COMMITTEE ON FOREIGN AFFAIRS
SUBCOMMITTEE HEARING NOTICE
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128**

**Subcommittee on Europe
Keith Self (R-TX), Chairman**

April 25, 2025

Revised

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Committee on Foreign Affairs to be held by the Subcommittee on Europe at 2:00 p.m. in Room 2200 of the Rayburn House Office Building. The hearing is available by live webcast on the Committee website at <https://foreignaffairs.house.gov/>.

DATE: Tuesday, April 29, 2025

TIME: 2:00 p.m.

LOCATION: 2200 RHOB

SUBJECT: Shaping the Future of Cyber Diplomacy: Review for State Department Reauthorization

WITNESSES:

Ms. Annie Fixler
Director, Center on Cyber and Technology
Foundation for Defense of Democracies

Ms. Latesha Love-Grayer
Director, International Affairs and Trade
U.S. Government Accountability Office

***** Mr. Theodore Nemeroff
Co-Founder and Vice President for Data and Compliance
Verific AI
~~Former Member, Policy Planning Staff~~
~~U.S. Department of State~~

*NOTE: Witnesses added/changed.

****NOTE:** Witnesses may be added.

By Direction of the Chair

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202-226-8467 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS
MINUTES OF EUROPE SUBCOMMITTEE HEARING

Day Tuesday Date April 29, 2025 Room 2200 RHOB

Starting Time 14:19 Ending Time 15:37

Recesses ☐ (___ to ___) (___ to ___) (___ to ___) (___ to ___) (___ to ___) (___ to ___)

Presiding Member(s)

Chairman Self

Check all of the following that apply:

Open Session ☒

Executive (closed) Session ☐

Televised ☒

Electronically Recorded (taped) ☒

Stenographic Record ☒

TITLE OF HEARING:

Shaping the Future of Cyber Diplomacy: Review for State Department Reauthorization

COMMITTEE MEMBERS PRESENT:

Attached

NON-COMMITTEE MEMBERS PRESENT:

None

HEARING WITNESSES: Same as meeting notice attached? Yes ☒ No ☐

(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

None

TIME SCHEDULED TO RECONVENE _____

or

TIME ADJOURNED 15:37

Meg Wagner
Full Committee Hearing Coordinator

Committee on Foreign Affairs
Subcommittee on Europe
119th Congress

ATTENDANCE

Meeting on: Shaping the Future of Cyber Diplomacy: Review for State Department Reauthorization
Date: April 29, 2025

[illegible]

**Questions for the Record Submitted to
Ms. Latesha Love-Grayer
Submitted by Rep. Gabe Amo
House Foreign Affairs Committee
April 29, 2025**

Question #1:

How has the firing of qualified workers affected the future ability of the State Department to attract talented workers in the cyber diplomacy workforce?

In January 2024, we reported that State officials said CDP needed to train existing staff and to hire more people to meet its growth plans.¹ We also noted that, at the time, CDP was (1) implementing and exploring additional mechanisms to address hiring needs and (2) working to develop partnerships with industry, academia, and other agencies to create a talent pipeline. However, during the course of our review, the head of CDP told us he recognized that competing with the private sector to hire staff with the right skill sets would be a challenge.

While we have not yet assessed the effects of proposed workforce changes on CDP's ability to meet its program goals, we have previously reported on the importance of strategic workforce planning. In our 2025 High Risk update, we stated that the government faces long-standing challenges in strategically managing its workforce, which has led to skills gaps in occupations, including in the cyber workforce.² Agencies experience skills gaps when they have an insufficient number of individuals or individuals without the appropriate skills or abilities to successfully perform their work. Federal agencies need to address skills gaps within the federal workforce by improving strategic workforce planning, training, and recruitment and retention efforts.

Strategic workforce planning, in particular, is critical when agencies undergo reorganization. Agencies need to ensure that any related workforce reductions do not produce skills gaps that could result in a failure to meet high-priority mission outcomes, deliver key services to the public, and consider unanticipated costs such as overtime and contracting.

We have received a broader request to examine the effects of staffing cuts at State and USAID and plan to begin new work on this issue soon.

¹GAO, *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*, [GAO-24-105563](#) (Washington, D.C.: Jan. 11, 2024).

²GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025).