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

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

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 infrastructure[10] 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 authorized[14] 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-Document-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 ad 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/usaid-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/d24105563.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 expertise[43] — 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.