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 can play 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.