Statement for the Record
Nathaniel Fick
Ambassador at Large for Cyberspace and Digital Policy
House Foreign Affairs Subcommittee on Indo-Pacific
January 17, 2024

Chairwoman Kim, Ranking Member Bera, and distinguished members of the Subcommittee, on behalf of the Department of State, thank you for the opportunity to speak with you today. I am honored to provide you with an overview of our work advancing U.S. technology policy priorities globally. I will also speak specifically to our efforts to strengthen U.S. technology leadership in the Indo-Pacific region.

At the State Department, I oversee the organizations that lead and coordinate the Department's work on cyberspace, digital policy, digital freedom, and emerging technologies: the Bureau of Cyberspace and Digital Policy, known as CDP, and the Office of the Special Envoy for Critical and Emerging Technology, S/TECH for short. Building on years of bipartisan work to establish these organizations, Secretary Blinken launched both in 2022 as part of a comprehensive effort to modernize American diplomacy and make technology issues more central to U.S. foreign policy.

I would like to thank the committee for your sustained, bipartisan support of this mission, particularly for the creation of a dedicated Cyberspace, Digital Connectivity, and Related Technology (CDT)-focused Foreign Assistance Fund in the recently passed 2023 State Department Authorization Act. Our assertiveness and demonstrated staying power are important around the world, and particularly in the Indo-Pacific, where visible U.S. presence, leadership, and assistance is an important element of our overall posture during this time of technology-focused geopolitical competition.

At our core, we believe in technology's power to solve major global challenges and support American and global prosperity. As a Marine combat veteran, an entrepreneur, and technology executive, and now the

inaugural Ambassador at Large for Cyberspace and Digital Policy, I see tech innovation as an increasingly foundational source of geopolitical power, driving more and more of what is, and is not, possible in our foreign and national security policies. Technology is now "the game," and we must engage in this geopolitical competition boldly and with urgency on behalf of our values and interests.

We face well-resourced and technologically capable competitors and adversaries who possess authoritarian visions and use long-term, technology-based strategies to advance those aspirations. These competitors most notably include the People's Republic of China (PRC), which wields all elements of national power to try to bend the rules-based international order in its favor, build economic and technical dependencies, and lock-in long-term influence. The PRC's efforts to use technology and government subsidies to export authoritarian precepts contrasts starkly with U.S. and allied views on the democratic development, deployment, and use of technology.

When governments wield technologies in irresponsible, and non-rights-respecting ways, my team and I work with the State Department's Assistant Secretary Kang, the Commerce Department's Assistant Secretary Kendler, and other colleagues across government to discourage, disincentivize, and counter the threats posed by such behavior. We do this by working together on sanctions, coordinating collaboration with international partners on critical and emerging technologies, and advancing U.S. priorities within multilateral organizations.

A key tenet of our team's work is building digital solidarity with allies and partners across the growing set of technology topics of high geopolitical significance: innovation and industry leadership, cyber incident response capacity building, information and communication technology (ICT) supply chain diversification, trusted digital infrastructure project support, and the rights-respecting uses of technology. This work cuts across the digital ecosystem from basic cybersecurity protections to 5G networks to other

aspects of digital infrastructure such as data centers, low-earth-orbit satellites, and undersea cables, as well as to the new generation of enabling technologies, including AI. In the Indo-Pacific, our work developing and stewarding these partnerships is extensive, covering nearly every country in the region.

Foreign assistance –and our partnership with U.S. Agency for International Development (USAID) – is an important element of our engagement on these topics. For example, we plan to leverage foreign assistance funding to support a major undersea cable and cybersecurity resilience project, together with Australia and private-sector partners, to connect strategically important Pacific Island countries and Small Island Developing States (SIDS) to trusted digital infrastructure. President Biden's announcement of a $15 million commitment to this project, subject to congressional approval, has already catalyzed additional discussions to expand the work – including additional funders, working with additional private partners, and expanding across the technology stack, from infrastructure, to cloud services, to dedicated cybersecurity provisions. I will be in the region next week to build on this work.

The creation of a dedicated Cyberspace, Digital Connectivity, and Related Technologies (CDT) Foreign Assistance Fund in the 2023 State Department Authorization Act is an important first step in streamlining work like this Pacific Island project, providing the U.S with the agility to move at the speed of technology, and the speed of our competitors. Funding this assistance instrument will be critical in establishing long-term investments in Indo-Pacific stability, increasing the security, resilience, and capacity of regional partners to protect themselves from threats, and pushing back against pervasive PRC influence and initiatives such as the Digital Silk Road.

Another example of our efforts to build digital solidarity in the region is the robust partnership between the United States and the Republic of Korea to disrupt DPRK revenue generation from IT workers, cryptocurrency heists, and illicit cyber activities. Since August 2022, the U.S.-ROK working group

has shut down thousands of DPRK accounts on freelance and payment platforms, issued cybersecurity advisories, sanctioned multiple DPRK-related entities, and built the capacity of other foreign partners to counter DPRK cyber threats.

More broadly, we have launched high-level dialogues on critical and emerging technologies with Singapore, the Republic of Korea, and India, together with the White House and interagency partners. These dialogues foster improved technology cooperation with strategic partners in areas including AI, biotechnology, and quantum computing. Last year, we strengthened our ties with Indonesia and Vietnam, with digital and cyber cooperation as key components of those enhanced relationships. This year, as another example, one of the key deliverables in the CDP-led U.S.-ASEAN Digital Work Plan is the *Responsible AI Roadmap* initiative, which will help Southeast Asia policymakers foster safe and inclusive AI ecosystems and complement ASEAN member states' efforts. This project is funded by CDP's foreign assistance work, implemented by USAID, and represents a good example of critical and emerging technology collaboration in the region.

We also engage closely, of course, with our Quad partners – Australia, Japan, and India – on critical and emerging technologies and the cybersecurity of our critical infrastructure. We support elements of the AUKUS security partnership with Australia and the United Kingdom, including work on the advanced capabilities component of that initiative - Pillar II. And later this month, I will represent the United States at the ASEAN Digital Ministers Meeting in Singapore to continue our engagement with ASEAN member states.

These activities represent just a small sample of the work the Department is doing to advance U.S. technology policy in the Indo-Pacific. Of equal importance, we are also strengthening U.S. diplomatic capabilities internally, across the State Department, to address these challenges in the future. We are on track to have a trained cyber and digital policy officer in virtually every U.S. mission around the world by the end of this year and are

continuously building new and enhanced training opportunities to upskill our collective workforce on cyber, digital, and emerging technology issues.

The United States, thanks to our robust innovation economy, is the world's leading provider of cybersecurity and digital technology products and services, including infrastructure, talent, and innovative applications from healthcare to defense, and from agriculture to financial services. The State Department works on behalf of the American people to promote cyber stability and trusted digital ecosystems around the world, including in the Indo-Pacific, creating opportunities for U.S. exports and jobs, maintaining U.S. leadership in these technologies, and ensuring enhanced security and trust in the digital domain.

Thank you for the opportunity to appear before you today. I look forward to answering your questions.