TESTIMONY OF

Iranga Kahangama
Assistant Secretary for Cyber, Infrastructure, Risk and Resilience
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

Tyrone Durham
Acting Director for the Nation State Threats Center
Office of Intelligence and Analysis
U.S. Department of Homeland Security

BEFORE

Committee on Homeland Security
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence
U.S. House of Representatives

ON

"A Security Sprint: Assessing the U.S. Homeland's Vulnerabilities to Chinese Communist Party Aggression"

May 23, 2023
Washington, D.C.

Chairman Pfluger, Ranking Member Magaziner, and distinguished Members of the Subcommittee, thank you for the opportunity to discuss critical work the Department of Homeland Security (DHS) is doing to combat the wide and multifaceted threat posed by the People's Republic of China (PRC). As the Administration's National Security Strategy states, and the National Cybersecurity Strategy reiterates, the PRC is our only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it. Consistent with this strategy and its pillar to invest in our strengths at home, DHS is leading efforts domestically to counter PRC threats to the homeland. We do this day in and day out with international, interagency, and private sector partners.

We must match our adversaries' determination through a whole-of-government response, with DHS playing a leading role on the front lines of that defense every day. Whether it is our work securing systems in cyberspace, investigating acts of transnational repression and transnational cybercrime, ensuring goods made from forced labor are not entering the country, or scrutinizing investments made in our companies and critical infrastructure, we take this mission seriously and with the highest attention.

Intelligence Assessment and Responsibilities

The PRC operates globally, using all instruments of national power to target the United States, and has a broad range of sophisticated intelligence capabilities. It continues to employ both overt and clandestine methods to undercut U.S. national security and economic security interests, such as stealing advanced and sensitive technologies using traditional and non-traditional collectors, amplifying narratives that sow doubt in U.S. institutions, and messaging against U.S. politicians it deems hostile. It also uses sister-city agreements, and other seemingly benign economic and cultural outreach to foster exploitable relationships, exert influence, and strengthen its foothold in the homeland. Recently, the PRC set up so-called "police stations" on U.S. soil to intimidate dissidents and other perceived adversaries.

Our homeland faces an array of complex threats from the PRC. In cyberspace, our interconnectedness and the technology that enables it exposes us to a dynamic and evolving threat environment that Beijing actively exploits, one that is not contained by borders or limited to centralized actors. The PRC also routinely bypasses law enforcement cooperation and extradition procedures and instead engages in transnational repression by using illegal tactics to surveil, threaten, and harass targets, both in person and digitally, around the globe. These activities directly violate the sovereignty of the host country and highlight that the PRC often lacks a legal basis for pursuing such targets. On economic security, the PRC abuses foreign investment and international trade by using illicit means to exploit this rules-based multilateral trading system in pursuit of a zero-sum approach to global competition that seeks to undermine American global leadership, national security, prosperity, and competitiveness.

DHS's Office of Intelligence and Analysis (I&A) is increasing intelligence collection and reporting on a wide range of potential threats and issues that the PRC poses to the United States, including threats within cybersecurity, counterintelligence, and transnational repression in the United States. This intelligence assists our partners in recognizing this activity, contributing to increased awareness of these threats by stakeholders who may be best positioned to identify and

mitigate the activities firsthand. I&A also produces strategic intelligence on threats to U.S. economic competitiveness, including intellectual property theft, supply chain threats, potentially harmful foreign investments, and illicit trade.

Cybersecurity

The PRC poses a highly advanced cyber threat to the homeland. It continues to leverage increasingly sophisticated, large-scale cyber espionage operations against the U.S. Government and a range of industries, organizations, and dissidents in the United States. The PRC uses cyber means to illicitly obtain U.S. intellectual property, personally identifiable information, and export-controlled information. PRC-backed malicious hackers, including those within the People's Liberation Army and the Ministry of State Security, are among the most active groups targeting governments and critical infrastructure, and the most active group targeting businesses around the globe. One PRC malicious hacking group, known as Advanced Persistent Threat 41, or APT41, has stolen intellectual property from at least 30 multinational companies in the pharmaceutical, energy, and manufacturing sectors, resulting in hundreds of billions of dollars of lost revenue. In addition to numerous state-affiliated APT groups, the PRC leverages a wide-ranging framework of laws to require all organizations operating in China—including joint ventures with foreign companies—to aid the regime in national intelligence efforts, with the obstruction of such efforts punishable under criminal law. This includes mandatory disclosure laws to compel organizations to report zero-day vulnerabilities, potentially leading to their exploitation before patching, and may punish companies when they do not comply.

To meet this challenge, the DHS Cybersecurity and Infrastructure Security Agency (CISA) publishes a variety of products to support organizations. Advisories, Alerts, and Malware Analysis Reports—frequently released in conjunction with other agencies and increasingly other countries—provide technical details on tactics, techniques, and procedures used by PRC state-sponsored cyber actors. For example, in October 2022, CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) released a joint-seal advisory outlining the top Common Vulnerabilities and Exposures used by the PRC since 2020. To mitigate against these types of threats, in October 2022, the Department released the Cybersecurity Performance Goals (CPGs), voluntary practices that outline the highest-priority baseline measures businesses and critical infrastructure owners of all sizes can take to protect themselves from malicious state actors and improve their overall defensive posture.

In the wake of PRC-affiliated APT Hafnium conducting broad exploitation of Microsoft Exchange Servers in 2021, CISA led asset response and mitigation efforts as part of the Cyber Unified Coordination Group that was stood up to combat this activity. Not only did CISA publish guidance to mitigate the group, but it also worked hand-in-hand with interagency partners and industry to ensure broad-based awareness and mitigation.

Public-private partnerships are another critical tool DHS uses to counter cyber threats and improve collective cybersecurity resilience. The DHS-led Cyber Safety Review Board (CSRB), a group made up of leading cyber experts in the public and private sectors, raised concerns about the PRC's mandatory vulnerability disclosure laws in the context of its review of the log4j vulnerability. Not only did the Board raise concerns about this law potentially affording the PRC

an exclusive window to take advantage of these vulnerabilities, it also noted possible sanctions placed on a company in the PRC for responsibly reporting a vulnerability to the wider cybersecurity community.

Likewise, CISA established the Joint Cyber Defense Collaborative (JCDC) in August 2021, which represents an evolution of the federal government's approach to operational collaboration and public-private partnerships. The JCDC is comprised of members of the interagency, private industry, and state, local, tribal, and territorial (SLTT) representatives to engage as co-equal partners in real time and persistent collaboration for operational outcomes. For example, in February 2022, a JCDC private sector member leveraged the Collaborative's operational relationships to alert two foreign governments that they were targets of novel PRC malware called Daxin. CISA was able to connect the government and the private sector company to assist in remediation in less than 48 hours, thanks to the strong public-private relationships of the JCDC.

DHS is also working closely with SLTT and interagency partners to improve our cybersecurity posture and protect our critical infrastructure. In July 2021, DHS launched StopRansomware.gov with the Department of Justice and other federal partners – the first whole-of-government website that pools federal resources to combat ransomware and helps private and public organizations of all sizes. In September 2022, CISA and the FBI built on this effort to launch the Joint Ransomware Task Force (JRTF) to coordinate a whole-of-government effort to combat the threat of ransomware. In September 2022, the Department announced the State and Local Cybersecurity Grant Program (SLCGP) to help SLTT partners address cybersecurity risks and cybersecurity threats to information systems. In Fiscal Year (FY) 2022, $185 million was made available under the SLCGP, with varying funding amounts allocated over four years from the Infrastructure Investment and Jobs Act.

Internationally, DHS is creating enduring partnerships with partners on cybersecurity, law enforcement, research and development, emergency management, and resilience. This includes the Secretary's participation in Singapore Cyber Week in October 2022, where he highlighted the risks of PRC-affiliated technology, and the signing a memorandum of cooperation on cybersecurity with Japan in January 2023. This agreement will allow Japanese agencies to strengthen operational collaboration with DHS, enhance the security of critical infrastructure, foster more opportunities for partnership, and continue sharing best practices with our Indo-Pacific partners. These alliances not only aid in countering malicious cyber activity from foreign adversaries, but also criminals who operate globally. For example, in January 2023, the FBI and the U.S. Secret Service, along with critical cooperation from international partners in Germany, the Netherlands, and Europol, were collectively able to dismantle the Hive ransomware group—a criminal operation that targeted more than 1,500 victims, including hospitals, schools, and critical infrastructure, across the globe.

Intellectual Property Rights (IPR) Theft

America's global leadership is underpinned by a fair, open, and competitive economy that cultivates opportunities and innovation at home and abroad. For too long, the PRC has exploited the rules-based multilateral trading system in pursuit of a zero-sum approach to global

competition while seeking to undermine American global leadership, national security, prosperity, and competitiveness. DHS plays an active role in securing the U.S. economy and its supply chains from PRC-related threats, through its various investigative authorities. DHS will continue to lead these efforts across our component missions to identify and mitigate foreign direct investment and surveillance risk while preserving the American-led order and ensuring fair and open global trade.

DHS works closely with interagency partners across several venues dedicated to protecting our national security and economic security, both operationally and in the ongoing development of national policy. We participate in robust, risk-based screening of inbound foreign direct investment via the Committee on Foreign Investment in the United States (CFIUS); advise the Federal Communications Commission (FCC) on the national security implications of foreign entities seeking U.S. licenses to operate communications critical infrastructure via the Committee for the Assessment of Foreign Participation in the U.S. Telecommunications Services Sector (known as Team Telecom); support the Commerce Department in exercising its authorities to assess broad risks to the information and communications technology supply chain from foreign adversaries; and lead the U.S. Government's response to stop global IP theft and enforce trade laws via U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI)-led National Intellectual Property Rights Coordination Center (IPR Center). These efforts derive their strength from the interagency approach, which brings together all relevant U.S. Government expertise on various technologies, industry sectors, and mission equities. DHS ensures these collaborative efforts benefit from our unique cybersecurity, critical infrastructure, and border security expertise.

For example, the United States has implemented carefully tailored restrictions on the most advanced semiconductor technology exports to China that are premised on national security concerns. HSI is expanding its efforts to counter the illicit acquisition of American microelectronics and other strategically important technology. These efforts include supporting the newly established Disruptive Technology Strike Force.

The Department has leveraged its authority within these interagency bodies to take significant steps to protect U.S. national and economic security from malign PRC activity. On October 26, 2021, the FCC revoked and terminated China Telecom America's (CTA) domestic and international Section 214 licenses in response to a joint recommendation from DHS and the Departments of Justice and Defense in their capacity as members of Team Telecom. This terminated CTA's ability to provide domestic and international telecommunications services within the United States. In addition to actions taken against PRC entities' ability to offer telecommunications services in the United States, the Department continues to leverage Team Telecom to address national security threats posed by the deployment of equipment from PRC vendors on critical telecommunications infrastructure, such as subsea fiber optic cables that carry most international communications traffic.

Forced Labor

The PRC's use of government-sponsored forced labor constitutes an economic threat against the United States and our international partners and undermines legitimate trade. In recent years, the PRC carried out what the United States has rightly characterized as a campaign of genocide against the predominantly Muslim Uyghurs and other members of ethnic and religious minority groups in the Xinjiang Uyghur Autonomous Region (Xinjiang) of western China.

The United States has long recognized the PRC's campaign constitutes a state-sponsored system of repression of these ethnic groups, and goods mined, produced, or manufactured, wholly or in part, with forced labor are unfairly traded goods that undermine the rule of law and threaten the economic security of legitimate businesses and their workers.

DHS has powerful tools in Section 307 of the Tariff Act of 1930 and the Uyghur Forced Labor Prevention Act of 2021 to prohibit the importation of goods made in whole or in part with forced labor. U.S. Customs and Border Protection is responsible for enforcing these laws, including by identifying and reviewing high-risk shipments, and detaining, excluding, or seizing and destroying merchandise determined to violate any forced labor prohibitions.

In its role as the Chair of the Forced Labor Enforcement Task Force, DHS leads the implementation and enforcement of these laws, while collectively leveraging the authorities and expertise of our sister agencies, including the Departments of State, Labor, Commerce, Justice, and Treasury, and the Office of the U.S. Trade Representative to develop initiatives that can support and enhance compliance.

Transnational Repression

The PRC threat is not limited to the economic or cyber domain. Operation Fox Hunt, a PRC government effort through which Beijing targets and seeks to repatriate and prosecute PRC individuals living in foreign countries whom the PRC alleges are guilty of corruption and should be returned to the PRC, has been used to target critics and dissidents living around the globe. Another recent example of the PRC's efforts to engage in acts of transnational repression is the PRC's unlawful operation of "overseas police service stations" in more than 50 countries, including the United States.[1] These acts no doubt represent only the tip of the iceberg of the PRC's transnational repression efforts in this country.

The PRC's repressive activities span far beyond U.S. borders and involve efforts to manipulate the rules and mechanisms of international law enforcement cooperation. Uyghur and other PRC diaspora communities in the United States have highlighted the detrimental impacts of politically motivated INTERPOL red notices issued at the request of the PRC government, which have resulted in the detention of community members overseas. DHS and its interagency partners have worked together over the last two years to strengthen the actions the U.S. Government is able to take in support of the internal INTERPOL reforms to prevent abuse of its critical tools for politically motivated purposes.

[1] See Safeguard Defenders September Report "Patrol and Persuade."

Another important aspect of DHS's strategy to counter transnational repression is its continuous engagement with targeted communities, which helps us to better understand the scope of the threat and respond appropriately. The PRC diaspora – including Uyghurs, Tibetans, and Hong Kongers – living in the United States often faces virtual harassment, threats, and attacks, including on social media platforms. Significantly, their family members in the PRC may face retaliation such as exit bans, loss of employment, and detention. DHS is working with members of affected communities to share information on federal resources available to support nationals in the United States and to support those seeking refuge in the United States.

At the Summit for Democracy in March, Secretary Mayorkas outlined new initiatives to counter the misuse of technology against communities who are at heightened risk of cyber threat targeting and transnational repression. CISA's High-Risk Community Protection Initiative, which is resourced by the JCDC, will focus initially on engaging civil society organizations to listen and learn about the cybersecurity threats they are facing, find out what support is most needed, identify positive work to amplify, and then work through the JCDC and with partners to fill cybersecurity gaps. Additionally, CISA, in coordination with the State Department, will cohost a Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression with the United Kingdom. At this dialogue, DHS will work with international partners from Australia, Canada, Denmark, Estonia, France, Japan, New Zealand, Norway, and the United Kingdom to improve the cybersecurity of civil society organizations, engage in information sharing on the threats facing high-risk communities, and identify opportunities for greater collaboration around the world.

Conclusion

In summary, the PRC poses a range of threats across different vectors to the United States and our homeland. However, DHS remains clear-eyed in our understanding of these multifaceted challenges and continues to proactively undertake efforts to mitigate risks to our nation's security and our democratic way of life. We remain unwavering in our commitment to counter the PRC's whole-of-government threat by providing a whole-of-homeland response, whether in cyberspace, in the defense of critical infrastructure, our economic security, or in preventing the assault on democratic values and freedoms.

Thank you for the opportunity to appear before you today and we look forward to taking your questions.