McCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY

CENTER FOR CYBER AND HOMELAND SECURITY

Testimony of Frank J. Cilluffo
Director, McCrary Institute for Cyber and Critical Infrastructure Security; and
Director, Center for Cyber and Homeland Security
Auburn University

Before the U.S. House of Representatives Committee on Transportation and Infrastructure

"The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors"

May 16, 2019

1301 Shelby Center, Auburn, AL 36849 | Tel: (334) 844 - 2209 | Fax: (334) 844 - 4487
mccrary.auburn.edu

Introduction

Chairman DeFazio, Ranking Member Graves, and distinguished Committee Members, thank you for the opportunity to testify before you today on a subject that is clearly of national importance. Your leadership in examining the impacts of foreign-owned enterprises on critical U.S. infrastructure and in the transportation sector in particular is commendable. The subject is as timely as it is concerning.

In this testimony, my goal is threefold: First, to offer a snapshot of the threat. Second, to place that threat in context by elaborating upon why it matters. And, third, to suggest a handful of feasible, impact-oriented policy recommendations that fall within the Committee's jurisdiction. However, before proceeding, I offer one caveat. Whereas other witnesses will focus deeply on the specifics of particular modalities of transportation and the impacts in connection thereto, my contribution will reside more at the strategic level. I will speak to the broader challenges, primarily the threats to critical U.S. infrastructure posed by foreign-owned enterprises and the response. This approach is intended to add value by acknowledging and emphasizing that the transportation sector must not be examined in isolation.

Pursuant to this approach, there are three chief concerns on the cyber side. One, the theft of information for the purpose of espionage or computer network exploitation, to include the mapping of critical U.S. infrastructure. Two, the theft of information to enable disruptive or destructive computer network attack, including hybrid cyber/physical attack. And, three, the insider threat, which cuts across all of these categories. In relation to foreign state-owned enterprises, it is also important to recognize that the potential threat is equally acute. It may arise deliberately with the foreign company acting as a willing conduit for its state of origin or inadvertently with the foreign company simply being subject in principle and/or by law of the state of origin to provide assistance upon request.

The State of Play: Risks to National & Economic Security

Foreign state-owned enterprises and China Railway Rolling Stock Corporation (CRRC) in particular is increasingly taking center-stage when it comes to building new rail cars for major American cities. Boston, Chicago, Los Angeles, and Philadelphia have each awarded contracts recently to CRRC, which placed markedly lower bids than the competition. The company is also expected to bid on upcoming rail-car contracts with the New York Metropolitan Transportation Authority, and the Washington (DC) Metropolitan Area Transit Authority.[1]

[1] Candice Norwood, "As China Builds Transit Cars for U.S. Cities, Congress Seeks to Ban Them," *Mass Transit* (March 19, 2019), https://www.masstransitmag.com/rail/vehicles/news/21072662/as-china-builds-transit-cars-for-us-cities-congress-seeks-to-ban-them

These procurement decisions and processes raise multiple concerns. First, the playing field is tilted: CRRC is able to underbid others because it benefits from state support.[2] Second, this support is just one element of a much broader strategy on China's part to challenge and undermine America economically.[3] Third, these economic factors are inextricably intertwined with U.S. national security because to undercut America's competitiveness is to damage the engine that powers our national security. And, fourth, CRRC's foothold in the supply chain of public transit to some of the largest cities in America effectively provides China with a wealth of intelligence, accessible through cyber means and vulnerabilities, among others. In military terms, such gathering of information for future exploitation and potential attack is called Intelligence Preparation of the Battlefield (IPB) — an important concept here, as China conceives of cyber, economic, military, and other measures as interconnected tools to achieve the country's larger geopolitical aims and ambitions. Looking beyond public transit and beyond China alone, the unfortunate reality that we must take as our operating assumption, is that U.S. critical infrastructures have already been mapped by our adversaries.

The situation is no less concerning in the air, where the use of unmanned aircraft systems (UAS) is becoming ever more common, for a range of purposes including surveying and securing large tracts of land. Notably, a Chinese manufacturer—DJI—has largely captured the American market for UAS. While UAS serve valuable functions, use of these Internet-connected systems entails risks. Most importantly, the using entity's sensitive data may be exposed and accessed.[4] This type of breach is especially problematic if the using entity supports a critical U.S. sector or function, and the manufacturer of the UAS is a foreign state-

[2] "CRRC has been winning U.S. procurements by bidding anywhere from 20 to 50 percent below bids from its non-subsidized, private sector competitors." Annie I. Anton and Justin Hemmings, "Recognizing Vendor Risks to National Security in the CFIUS Process, *Lawfare* (January 4, 2019), https://www.lawfareblog.com/recognizing-vendor-risks-national-security-cfius-process

[3] As explained by a senior official at the U.S. Department of Justice just last month: "The problem is not that China is working to master critical technologies, or even that it is competing with the United States, but rather the means by which it is doing so. 'Made in China 2025' is as much a roadmap to theft as it is guidance to innovate. Since the plan was announced in 2015, the Justice Department has charged Chinese individuals and entities with trade secret theft implicating at least eight of the ten sectors [identified as 'strategic manufacturing industries for promotion and development' by the Made in China 2025 strategy]. Over a longer time period, since 2011, more than 90 percent of the Department's economic espionage prosecutions (*i.e.*, cases alleging trade secret theft by or to benefit a foreign state) involve China, and more than two-thirds of all federal trade secret theft cases during that period have had at least a geographical nexus to China. Some of those cases demonstrate that China is using its intelligence services and their tradecraft to target our private sector's intellectual property. In the space of two months last year, the Department announced three cases alleging crimes by the same arm of the Chinese intelligence services, the Jiangsu Ministry of State Security, also known as the 'JSSD'." "Deputy Assistant Attorney General Adam S. Hickey of the National Security Division Delivers Remarks at the Fifth Annual Conference on CFIUS and Team Telecom," (April 24, 2019), https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-national-security-division-delivers-0

[4] "In 2017, U.S. customs authorities alleged that drones produced by Chinese company DJI, which has dominated the U.S. and Canadian drone markets, likely provided China with access to U.S. critical infrastructure and law enforcement data. DJI denied the allegation." Matthew Pennington, "US panel warns against government purchase of Chinese tech," *The Associated Press* (November 14, 2018), https://www.fifthdomain.com/critical-infrastructure/2018/11/14/us-panel-warns-against-government-purchase-of-chinese-tech/

owned enterprise. Chinese companies, for example, may be legally required to help advance the mission and goals of China's security and intelligence services. The use of UAS also raises the prospect of cyber/physical convergence, whereby cyber tools and operations may be invoked (particularly by an adversary with hostile intent) to generate kinetic or real-world consequences. Notwithstanding this background, the UAS issue has yet to receive in this country the attention and commensurate timely action that this concerning matter deserves.

Within the transportation sector alone, the potential vulnerabilities are manifold. Public transit, freight rail, UAS, seaports, and so on — each presents a tempting target on its own.[5] At the same time however, these transport hubs in surface, air and maritime also individually and collectively support and enable the U.S. military to achieve its ends and operations both at home and abroad. The ability of U.S. forces to complete these activities successfully and in service of the national interest is what the U.S. defense community refers to as Mission Assurance. Continuity of these operations, and resilience in the face of disruptive or destructive events, is of fundamental importance. National defense priorities thus intersect and, to a certain extent, depend upon the integrity of the transportation sector. If the latter is compromised that may put Mission Assurance at risk, since logistics are the lifeblood of the U.S. military; and to hamper that planning and execution is to jeopardize our ability to deploy forces and prosecute war. Put differently, the impacts of foreign state-owned enterprises on the transportation sector range well beyond the economic and stray deeply and directly into the realm of national security. Again, the potential for cyber/physical convergence, with resulting consequences on the battlefield, is concerning. Indeed, the Center for Cyber and Homeland Security will be releasing a report shortly entitled "Strengthening Defense Mission Assurance Against Emerging Threats." We will make it available to the Committee.

Foreign state-owned enterprises and the advanced technologies that they offer, often at highly competitive prices and frequently accompanied by additional concessionary financing, present a dilemma for other critical infrastructure sectors, too. 5G telecommunications technology proffered worldwide by Chinese companies Huawei and ZTE is a clear and prominent example. 5G will be the foundation upon which next-generation networks, globally, will rest. Currently, countries are in the process of selecting the entities that will build and contribute to that foundation. This is a seminal decision that will affect not only the telecommunications sector in each country, but all of the other sectors that the telecommunications industry supports and services (such as transportation — including autonomous vehicles where the cyber domain meets and melds with the physical world).

As such, 5G will be the hub powering many spokes that in turn may be critical sectors or functions. To be selected a preferred provider of the components for the hub is a tremendous

[5] "State and local government agencies have become increasingly vulnerable to cyberattacks — particularly when it comes to public transportation. In 2016, hackers hit the San Francisco transit system with a ransomware attack demanding $70,000. The following year, Sacramento Regional Transit faced a similar strike. In 2018, the Colorado Department of Transportation shut down 2,000 computers after falling victim to two ransomware attacks in two weeks." Norwood, https://www.governing.com/topics/transportation-infrastructure/gov-china-crrc-congress-cities-transit-federal-funding-bill.html

economic opportunity. Huawei and ZTE are therefore competing aggressively to act as suppliers, including to the United States. Based on evidence of these companies' complicity with the Chinese government, and the national security concerns that this raises (e.g., espionage, IPB, intellectual property theft, etc.), the United States has rejected these overtures, and urged its allies and partners to do the same.[6] While paths forward may ultimately diverge, the U.S. way ahead is clear, and it will not engage Huawei or ZTE. Significantly, the strategic significance of 5G, as the bedrock upon which telecommunications and so much more will rely, has also been recognized by more than 30 countries, which met recently in Prague, and produced a series of principles regarding the "cyber security of communications networks in a globally digitized world."[7]

Other products and technologies supplied by Chinese companies that have raised security concerns in the United States include cameras, such as video surveillance equipment, manufactured by Hangzhou Hikvision Digital Technology. The company, a global giant in its field, began as a Chinese government research institute. Today, three Chinese state-owned enterprises retain a large ownership stake of more than 40 percent in the company. Nevertheless, Hikvision cameras have been used in U.S. prisons and schools, and "sensitive sites such as the Fort Leonard Wood army base and the U.S. embassy in Kabul." Hikvision has also been the subject of allegations that the company maintains access to its devices "even if you change the admin [passwords] and the firewall."[8]

Many other smaller but still important opportunities exist for foreign state-owned enterprises to make inroads into U.S. critical infrastructure either directly or indirectly. Flush with the financial backing of their state sponsors, these foreign proxy entities can step in and scoop up U.S. assets and entities that are on the verge of bankruptcy or in need of start-up capital.[9] Such acquisitions may relate to a niche or component that may seem minor to the untrained eye,

---

[6] Frank J. Cilluffo and Sharon L. Cardash, "What's wrong with Huawei, and why are countries banning the Chinese telecommunications firm?" *The Conversation* (December 19, 2018), https://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036. Note also, "the potential impact of malicious cyberattacks…will intensify with the adoption of ultra-fast 5G networks that could quicken data speeds by up to 100 times." Pennington, https://www.fifthdomain.com/critical-infrastructure/2018/11/14/us-panel-warns-against-government-purchase-of-chinese-tech/

[7] Government of the Czech Republic, "Prague 5G Security Conference announced series of recommendations: the Prague Proposals," (May 3, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

[8] Sidney Leng, "China's Hikvision hits out at US Congress over 'baseless' ban on using surveillance equipment over national security concerns," *South China Morning Post* (May 27, 2018), https://www.scmp.com/news/china/diplomacy-defence/article/2148010/chinas-hikvision-hits-out-us-congress-over-baseless-ban

[9] The U.S.-China Economic and Security Review Commission notes that China was "the largest single foreign VC [venture capital] investor ($24 billion) in the United States cumulatively between 2015 and 2017, according to a recent U.S. government study." *2018 Report to Congress* (November 2018), https://www.uscc.gov/sites/default/files/annual_reports/2018%20Annual%20Report%20to%20Congress.pdf at page 30. See also: Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation* (January 2018), Defense Innovation Unit Experimental (DIUx) Report.

but may bear significant import. Consider switches, for instance. They play a crucial role in freight and passenger rail, and the ability to alter their activation or operation could cause substantial harm to both persons and property. Nor would such alteration be necessary to perform in person or onsite. Instead, tampering could take place from afar through silent and stealthy cyber means.

This scenario also highlights the criticality of time, as invoked by the phrase Positioning, Navigation, and Timing (PNT). Accuracy of time and the positioning and navigation functions that it enables is too often overlooked, underplayed, or taken as given. We do so at our peril. Here again, China is investing heavily with the dual goals of enhancing its ability to safeguard its own PNT and undermine others, such as through anti-satellite capabilities that could blind and bind the U.S. military. Modern militaries rely heavily on space-based assets for their transit and targeting requirements and other needs, thereby expanding the potential surface of attack. In addition, the continued expansion of the Internet of Things and the related number of connected devices worldwide that are giving us smart cities, smart cars, and sensors galore, likewise serves to increase exponentially both vulnerabilities and possibilities for attack. Heightened functionality comes at a price for soldiers and consumers alike.[10] The ever-present criticality of PNT functions and the coming ubiquity of 5G technology each underscore the need to remain resilient, including by considering alternatives to our heavy reliance on the space-based Global Positioning System (GPS), as a precautionary measure.

Supply chain concerns are by no means limited to goods or services of Chinese origin.[11] Software produced by the Russian anti-virus company Kaspersky Lab is the subject of a ban on use by U.S. federal agencies. Kaspersky Lab's leadership has close ties to Russia's leadership, and the Lab may be legally obligated to assist Russian security and intelligence officials with espionage efforts directed against the U.S. government.[12] Indeed, even if the assist to foreign state officials in Moscow, Beijing, or elsewhere, were inadvertent or unwitting on the part of the foreign supplier, the possibility for that enterprise and its products, technologies and services to serve as conduit is simply unacceptable.

---

[10] "`The scale of Chinese state support for the IoT, the close supply chain integration between the United States and China, and China's role as an economic and military competitor to the United States creates enormous economic, security, supply chain, and data privacy risks for the United States…'". Pennington, https://www.fifthdomain.com/critical-infrastructure/2018/11/14/us-panel-warns-against-government-purchase-of-chinese-tech/ [citing the 2018 Report of the U.S.-China Economic and Security Review Commission]

[11] But note: "the U.S. government depends on commercial, off-the-shelf products, many of them made in China, for more than 95 percent of its electronics components and information technology systems." Pennington, https://www.fifthdomain.com/critical-infrastructure/2018/11/14/us-panel-warns-against-government-purchase-of-chinese-tech/. Moreover: "An analysis of seven major U.S. based tech companies — HP, IBM, Dell, Cisco, Unisys, Microsoft and Intel — found that more than half of the products they and their suppliers use are shipped from China." Derek B. Johnson, "China's penetration of U.S. supply chain runs deep, says report," *FCW* (April 23, 2018), https://fcw.com/articles/2018/04/23/china-supply-chain-cyber.aspx?m=1

[12] Joseph Marks, "Government's Kaspersky Ban Takes Effect," *Nextgov* (July 16, 2018), https://www.nextgov.com/cybersecurity/2018/07/governments-kaspersky-ban-takes-effect/149758/

Despite measures like the Kaspersky software ban that are intended to mitigate harm to U.S. national security, the imprint of foreign state-owned enterprises upon critical U.S. infrastructure today remains troubling. Consider the grid. According to the deputy director of counterintelligence at the Department of Energy, more than 200 Chinese transformers have come into the U.S. energy sector during the past decade. Previously there were none.[13] The groundwork for future sabotage, actioned remotely by digital means, is now in place.

In some instances, the problem is low-tech, at least on its face. A recent GAO report revealed that just six TSA employees were responsible for overseeing the security of 2.7 million miles of oil & gas pipeline.[14] This is patently insufficient, regardless the degree of foreign state-owned enterprise involvement in this area. The problem appears to be compounded by shortfalls in cybersecurity expertise on the part of relevant personnel, and this further inhibits robust oversight at a time when pipeline operations are increasingly computerized.

In short, we have failed to inoculate ourselves against the many and varied threats to U.S. critical infrastructure posed by nation-state actors and their proxies. This, despite the fact that our adversaries have demonstrated their interest year after year in mapping our architectures and engaging in persistent computer network exploitation efforts that have no benign purpose and could ultimately be combined with kinetic measures. China and Russia are not alone in these pursuits. Iran and North Korea join them and possess a degree of hostile intent that more than makes up for any shortfalls in their respective capacities and capabilities. In this regard, we ought not to forget Iran's past cyber-targeting of U.S. banks (DDoS attacks) or its cyber-foray into the workings of a New York State dam.[15] The 2018 Foreign Economic Espionage in Cyberspace Report produced by the National Counterintelligence and Security Center notes also, "Iranian hackers target U.S. aerospace and civil aviation firms."[16] Nor should we forget North Korea's destructive cyber-attack on Sony Pictures Entertainment.[17]

[13] Blake Sobczak and Peter Behr, "China and America's 400-ton electric albatross," *E&E News* (April 25, 2019), https://www.eenews.net/stories/1060216451

[14] Catalin Cimpanu, "Only six TSA staffers are overseeing US oil & gas pipeline security," *ZDNet* (May 2, 2019), https://www.zdnet.com/article/only-six-tsa-staffers-are-overseeing-us-oil-gas-pipeline-security/

[15] Dustin Volz, Nate Raymond, Jim Finkle, "U.S. to charge Iran in cyber attacks against banks, New York dam – sources," *Reuters* (March 23, 2016), https://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WP2NM

[16] National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf at page 9. In respect of Russia, the Report notes further (at page 8): "Moscow has used cyber operations to collect intellectual property data from U.S. energy, healthcare, and technology companies. For example, Russian Government hackers last year compromised dozens of U.S. energy firms, including their operational networks. This activity could be driven by multiple objectives, including collecting intelligence, developing accesses for disruptive purposes, and providing sensitive U.S. intellectual property to Russian companies."

[17] Peter Elkind, "Inside the Hack of the Century," *Fortune* (June 25, 2015), http://fortune.com/sony-hack-part-1/

Proposed Response: Selected Action Recommendations

The magnitude of the challenge is daunting, but there are steps that we can and should take in order to confront and counter the array of threats and problems that prevail, particularly those of highest potential consequence. What we cannot afford to do is grind the U.S. economy to a halt by introducing blanket and overly blunt security measures. Instead, we must tailor and calibrate our responses to limit any collateral damage to U.S. interests, separate and apart from national security concerns. In practice, this means working to elevate security concerns, monitor them, test our responses, and continually refine those regimes. Admittedly, this is a tall order. But, like any complex task, it can be broken down into a series of steps to be taken in a sequence that deals with first things first:

Prioritize Lifeline Sectors and National Critical Functions. If everything is critical then nothing is, and since we cannot protect everything, everywhere, all the time, we must focus our limited human, capital and other resources on those assets and operations whose takedown or undermining would be most damaging to the nation. Put differently, we must manage risk since we cannot eliminate it. To this end, a good place to start would be to direct our attention to the so-called "Lifeline" Sectors, which have already been identified as the most critical of the critical. These include the defense industrial base, energy, financial services, transportation, telecommunications, and water. In addition, the list of National Critical Functions (NCF) recently released by the National Risk Management Center, nested within the Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA), provides another series of guideposts for prioritization. The NCF list addresses cross-sector and system-wide risks, and thereby complements a focus on lifeline sectors, by taking the logical next step, which is aligning and calibrating the most critical of sectors and the most critical of functions.

Know and Scrutinize Your Supply Chain. It should be patently clear from the above-described state of play that any entity is only as strong as the weakest link in its chain. In the context of business operations or government enterprise, this means that knowing and scrutinizing your supply chain is a prerequisite to public safety and security. However, while few would argue with this statement as a matter of principle, not enough businesses or government officials and contractors are paying this principle the heed that it deserves in practice. Instead of acting according to the old adage, "trust but verify," too many of us are relying on trust alone[18]. In the context of critical infrastructure, this could have catastrophic consequences. Executive Order 13806 on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States[19] was assuredly a helpful initiative in this respect as was the Department of Defense-led Interagency Task Force Report[20] and, the Information

[18] Phil Muncaster, "Most Firms Rely on Trust Alone for Supply Chain Security," *Infosecurity Magazine* (May 1, 2019), https://www.infosecurity-magazine.com/news/most-firms-rely-trust-alone-supply-1/

[19] (July 21, 2017), https://www.federalregister.gov/documents/2017/07/26/2017-15860/assessing-and-strengthening-the-manufacturing-and-defense-industrial-base-and-supply-chain

[20] Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the*

and Communications Technology (ICT) Supply Chain Risk Management Task Force launched recently by DHS CISA.[21] However, it is incumbent upon all of us to widen and deepen the effort.[22]

Empower CFIUS to better Protect Critical U.S. Infrastructure. The Committee on Foreign Investment in the United States (CFIUS) is an interagency body mandated to review the national security implications of certain transactions. Taken together with the 2018 *Foreign Investment Risk Review and Modernization Act*, and our export control regime, we have in place an architecture and mechanisms to assess and thwart significant, negative consequences for U.S. national security that might arise from foreign investment or technology transfer. The system in place entails evidence-based inquiry and analysis but contains some important gaps. These are identified and discussed in specific bilateral context in a staff research report of the U.S.-China Economic and Security Review Commission released earlier this month. The report includes the concern that "investments in U.S. critical technologies based outside the United States" fall beyond the detection ambit of CFIUS.[23]

Develop Strategy, Not Just Tactics, and Integrate Cyber. American economic advantage, military strength, innovation, jobs and many other important national equities are at stake.[24] There is a resultant compelling need to address the ecosystem of threats in a comprehensive and contextualized manner that balances and accommodates the tensions that may exist among the various equities at play. At the same time, cybersecurity factors, such as risk assessments and risk management strategies, should be woven into strategy at inception and across the board, rather than treated as a separate vertical, that must be retrofitted. To these ends, a domestic version of The Prague Proposals, which are principles regarding the "cyber

---

United States (September 2018), https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

[21] Robert Kolasky, Statement for the Record for a Hearing on "Securing U.S. Surface Transportation from Cyber Attacks," before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation (February 26, 2019), https://homeland.house.gov/sites/democrats.homeland.house.gov/files/documents/Testimony-Kolasky.pdf at page 5

[22] Late last year, the Senate passed legislation to stand up an interagency council to "develop rules of the road for federal supply chain security." Derek B. Johnson, "Senate passes bill to establish governmentwide supply chain council," *FCW* (December 19, 2018), https://fcw.com/articles/2018/12/19/senate-supply-chain-bill-johnson.aspx?m=1. The subsequently enacted *SECURE Technology Act* established the Federal Acquisition Security Council. See *H.R. 7327* (January 3, 2018), at *Title II*, https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Law-BILLS-7327.pdf

[23] Sean O'Connor, *How Chinese Companies Facilitate Technology Transfer from the United States*, U.S.-China Economic and Security Review Commission Staff Research Report (May 6, 2019), https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2019/may/cs05072019_China_Tech_Transfer.pdf at page 10. Also, as noted in the 2018 Foreign Economic Espionage in Cyberspace Report: "China uses front companies to obscure the hand of the Chinese government and acquire export controlled technology." https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf at page 6.

[24] The list is illustrative, not exhaustive, and elaborated by the National Counterintelligence and Security Center. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

security of communication networks in a globally digitized world" generated at the recent 5G Security Conference in which 32 countries participated, could prove useful for safeguarding U.S. Lifeline Sectors and National Critical Functions in connection with the widespread rollout and implementation of 5G technology.[25]

Make Building the Cyber Workforce and a Network of Critical Technologies Testbeds National Imperatives. Report after report has identified large shortfalls in the supply of skilled cyber professionals relative to U.S. demand for them in both the public and private sectors. Yet, cyber practitioners are crucial to identifying, assessing, and responding to the threat as manifested and previously described. For government, the under-supply problem is magnified because private industry can offer prospective and existing employees greater salary and benefits. Although psychic income derived from the government mission of serving the national interest is a significant pull and retention factor, the fact remains that the pool of qualified candidates is itself too small. It must be expanded, urgently, to address the deficit of knowledge and bandwidth that is needed in our public institutions and in our companies to counter and thwart cyber threats posed by state actors to U.S. critical infrastructure. The recent Executive Order on America's Cybersecurity Workforce recognizes this challenge,[26] but continued and whole-of-society efforts will be required. In addition, on the technology side, we lack a strategic approach to integrating advancements into the broader ecosystem. An R&D effort, in the form of a nationwide network of technology testbeds that simulate a realistic pan-sectoral environment, is needed to remedy this shortfall. Taken in aggregate, such a platform would identify and explore the various national and economic security implications of new and critical technologies before they are in widespread use.

Conclusion

National security and free markets need not be an either/or proposition — we need both. With leadership and sustained determination on the part of both government and industry, complemented and supported by robust partnership of the two, we can meet that goal. Thank you again for the opportunity to appear before you today. It is a privilege to contribute to this important conversation and analysis,[27] and I look forward to trying to answer any questions that you may have.

[25] Government of the Czech Republic, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/

[26] (May 2, 2019), https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

[27] I would be remiss if I did not thank the deputy director of the Center for Cyber and Homeland Security, Sharon L. Cardash, for her skillful assistance in preparing this testimony.