AUBURN UNIVERSITY

McCRARY INSTITUTE FOR
CYBER AND CRITICAL
INFRASTRUCTURE 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 United States Senate Committee on Banking, Housing, and Urban Affairs

"Threats Posed by State-Owned and State-Supported Enterprises to Public Transportation"

March 5, 2020

1214 Shelby Center, Auburn, AL 36849 | Tel: (334) 844 - 2209 | Fax: (334) 844 - 4487
mccrary.auburn.edu

Introduction

Chairman Crapo, Ranking Member Brown, and distinguished Committee Members — notably including Senators Shelby and Jones from my Institute's home State of Alabama — thank you for the opportunity to testify before you today.

The threats to public transportation posed by State-owned and State-supported enterprises is a matter of national significance, as the issue bears on U.S. national and economic security, which are inextricably intertwined. Your leadership in this area is important and commendable, not least because the concerns that are at play in regards to public transportation apply also to other critical U.S. infrastructure sectors and national critical functions.[1]

Fortunately, the subject under study today has been the focus of considerable attention on the part of lawmakers in recent months. Much credit is, of course, due to this Committee's Chairman and Ranking Member, together with Senators Cornyn and Baldwin (also testifying today), for leading the charge on legislation in this area.[2]

By way of further example, last May, your colleagues on the House of Representatives' Committee on Transportation and Infrastructure also convened a hearing similar to this one, at which I also had the privilege of testifying.[3] My statement before you today builds on my statement of last year, and I will take a parallel approach: first, I will set out the threat and place it in context, showing why it matters; and second, I will offer selected policy recommendations that speak to priority issues requiring timely action.

The Threat Climate and Its Implications

This hearing speaks specifically to the threat posed to public transportation by State-owned and State-supported enterprises. On this question, let me speak plainly: the chief threat comes from China and certainly includes the sale and provision of railway cars to U.S. transit systems — but the threat also extends far beyond, to much more than the transportation sector alone.

The crux of the matter is that State-owned and State-supported enterprises are able to outbid others when competing for contracts. In the case of China, a non-market economy, this is part of a broader strategy to undermine America's economic might; and the challenge is not just

---

[1] The National Risk Management Center (NRMC) has identified and created a list of National Critical Functions that addresses cross-sector and system-wide risks. NRMC is nested within the Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA). For details, see https://www.cisa.gov/national-critical-functions.

[2] S. 846, *Transit Infrastructure Vehicle Security Act*, https://www.congress.gov/bill/116th-congress/senate-bill/846/cosponsors?searchResultViewType=expanded&KWICView=false

[3] "The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors," (May 16, 2019), http://cchs.auburn.edu/_files/the-impacts-of-state-owned-enterprises-on-public-transit-and-freight-rail-sectors.pdf. This statement should be read in tandem with the present written testimony, since I have not repeated all of the details here.

economic. This is so because U.S. national and economic security are inextricably interwoven. Each depends upon the other.

From a cyber-standpoint, a State-owned enterprise (Chinese or otherwise) foothold into the supply chain of public transportation, a critical U.S. infrastructure sector, could open the door to a wealth of intelligence that could be weaponized against us. While there are a multitude of ways to engage in espionage, the line between it (computer network exploitation) and computer network attack is thin and turns largely on intent. Put differently, if you can exploit, you can also attack, if the will exists to do so.

This begs the question, why open this door to espionage as potential gateway for attack, if it is not necessary to do so?[4] Keep in mind that espionage in this context could allow an adversary to map critical U.S. infrastructure prior to attack and otherwise engage in intelligence preparation of the battlefield (as the military would say). While, in general, security is not the only factor to be considered in decision-making in this context public safety should be the larger concern, especially given the potential for hybrid (not just cyber but physical) consequences.

In case the above is a bit too abstract to appreciate fully, let me explain more concretely the cybersecurity risks associated with railcars produced by State-owned enterprises: the potential for continuous and purposeful (adversary) access to our railcar/transit systems may arise through equipment communications links; hardware or software may be compromised; and the likelihood of direct access is real.[5]

Consider just some of the consequences that could follow from these risks: the adversary could shut down trains and disrupt transit operations; knock-on effects could hit other critical U.S. infrastructure sectors; and major U.S. cities that depend strongly on rapid transit systems could experience significant economic effects, particularly if an incident were to disrupt systems for a lengthy period.

It is important to note that State-owned and State-supported enterprises may not even be witting accomplices in any of this. While certain countries (such as China and Russia) have laws that require State-owned enterprises to furnish assistance upon request,[6] such companies may also be inadvertent conduits for furthering the goals and ambitions of their (authoritarian) State of origin.

Despite this array of serious security implications, America has yet to inoculate itself against them. I will not repeat here all of the case-specific evidence offered in my 2019 testimony.

---

[4] To be clear on the issue of necessity in the context of railcars in particular, there do exist alternatives for U.S. transit systems to pursue instead of purchasing from Chinese State-owned or State-supported enterprises. See below for additional details.

[5] Via onsite employee (State-owned enterprise employee or contractor sited at U.S. transit agency) with access to networks/operations.

[6] In the case of China, at least three instruments are at play: the National Intelligence Law of 2017, the associated Implementing Regulations, and Communist Party requirements enshrined in law and iterated publicly in 2014, 2015, and 2017. For details, see Nick Eftimiades, "On the Question of Chinese Espionage" (forthcoming), *Brown University Journal*.

Suffice it to say, for the sake of illustration, that China Railway Rolling Stock Corporation (CRRC) is building new rail cars for major American cities such as Boston, Chicago, Los Angeles, and Philadelphia. This gives rise to a plethora of vulnerabilities as described.

The temptation to procure from CRRC is understandable from the perspective of cost alone; State subsidies tilt the playing field heavily in China's favor.[7] But there is so much more than price at play here: China is not just seeking to win in U.S. markets[8]; it has developed and is executing a much larger strategy (Made in China 2025[9]) designed to further the country's economic, military, and political goals.

A forthcoming analysis of 464 documented cases of China's espionage worldwide concludes that "collection efforts coordinate closely to the priority technologies identified in government strategic planning documents," including Made in China 2025, and Space Science and Technology in China: A Road-map to 2050. Chinese "private companies" and State-owned enterprises each engage in or support espionage in just over 21 percent of the cases studied; and together constitute slightly more than 43 percent of the case total. Targets include "U.S. military and space technologies" and "commercial interests."[10]

Put bluntly, China's strategy is powered by theft of U.S. intellectual property; and we ignore or underplay that broader context at our peril. In the words of the new U.S. National Counterintelligence Strategy released last month by the National Counterintelligence and Security Center: "A more powerful and emboldened China is increasingly asserting itself by

---

[7] For a long-form examination of a case of Chinese underbidding giving rise to quality control concerns and costs that ultimately "ballooned" see: Charles Piller, "Troubled welds on the Bay Bridge: How a Chinese builder's flaws left structural doubts and cost taxpayers," The Sacramento Bee (June 7, 2014), https://www.sacbee.com/news/investigations/bay-bridge/article2600743.html

[8] Even in relation to the narrow issue of trying to win in U.S. markets however CRRC has been engaged in a "misinformation campaign" — as noted in a compelling letter of warning to Secretary of Transportation Elaine Chao (dated February 13, 2020) from Senators Cornyn and Baldwin. In the Senators' words: "The CRRC has used the argument that no U.S. companies manufacture transit railcars and if not for CRRC we would have no railcars in America. This…does not take into account that the U.S. has a thriving and robust transit rail manufacturing sector... which is comprised of numerous enterprises from market economy allies of the U.S.…Most importantly, unlike CRRC…, these companies use U.S. supply chains, use U.S. produced components, and are compliant under 'Buy America' provisions." https://www.documentcloud.org/documents/6781588-Cornyn-Baldwin-TIVSA-Implementation.html

[9] "The Made in China 2025 Initiative: Economic Implications for the United States," Congressional Research Service – *In Focus* (updated April 12, 2019), https://fas.org/sgp/crs/row/IF10964.pdf. In a 2018 speech to China's National Academy of Sciences and Engineering, President Xi Jinping asserted: "If China is to flourish and rejuvenate, it must vigorously develop science and technology and strive to become the world's major scientific center and innovative highland. … Self-reliance is the basis for the struggle of the Chinese nation to stand on its own footing in the world." Cited in Simon Sharwood, "Chinese president Xi seeks innovation independence," *The Register* (June 1, 2018), https://www.theregister.co.uk/2018/06/01/xi_xinping_science_technology_policy_speech/

[10] Eftimiades, "On the Question of Chinese Espionage." Note also: Department of Justice Office of Public Affairs, "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China" (July 11, 2019), https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china ["A software engineer at a suburban Chicago locomotive manufacturer stole proprietary information from the company and took it to China"].

stealing our technology and intellectual property in an effort to erode United States economic and military superiority."[11]

The scale and scope of the challenge is daunting. According to FBI Director Christopher Wray, "`The FBI has about a thousand investigations involving China's attempted theft of U.S.-based technology in all 56 of our field offices and spanning just about every industry and sector'." U.S. companies and U.S. universities are both targets — "all over the country, from Alabama to Iowa."[12] The situation is all the more concerning when set against China's plans to double its current spending on research ($400 million) to $800 million. It is expected that these monies will be directed primarily to the country's Thousand Talents Program (for recruitment) and the buy-out of bankrupt companies.[13]

In addition, economic and political power are (of course) tightly connected. As press reports note, "China's influence playbook centers around economic leverage stemming from its growing wealth." The FBI's Foreign Influence Task Force notably includes a unit dedicated to "countering China's political influence in the United States."[14]

Against this backdrop, the new U.S. National Counterintelligence Strategy articulates five Strategic Objectives that require a whole-of-society approach, including the following that are of particular relevance to today's hearing: Protect the Nation's Critical Infrastructure; Reduce Threats to Key U.S. Supply Chains; and Counter the Exploitation of the U.S. Economy.

Returning specifically to transportation, against this broader background, rail is not the only concern: by way of further example, a Chinese manufacturer (DJI) has captured the U.S. market for unmanned aircraft systems (UAS).[15] The end-user of these systems may be a range of critical U.S. infrastructure sectors, and sensitive data may be exposed.[16]

---

[11] *National Counterintelligence Strategy of the United States of America 2020-2022*, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf

[12] Catalin Cimpanu, "FBI is investigating more than 1,000 cases of Chinese theft of US technology," *ZDNet* (February 9, 2020), https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/. Note also, the FBI "made 19 arrests this fiscal year alone on charges of Chinese economic espionage. In comparison, the FBI made 24 arrests all last fiscal year, and only 15, five years earlier, in 2014." *Ibid*. See also: Jackson Cote, "`China's economic espionage and theft is a real,'[*sic*] U.S. Attorney Andrew Lelling says after arrest of Harvard professor for undisclosed ties to China," *MassLive.com* (January 28, 2020), https://www.masslive.com/boston/2020/01/chinese-economic-espionage-and-theft-is-a-real-us-attorney-andrew-lelling-says-after-arrest-of-harvard-professor-for-undisclosed-ties-to-china.html

[13] Telephone interview with Nick Eftimiades on February 18, 2020.

[14] Bethany Allen-Ebrahimian, "Exclusive: How the FBI combats China's political meddling," *Axios* (February 12, 2020), https://www.axios.com/fbi-china-us-political-influence-0e70d07c-2d60-47cd-a5c3-6c72b2064941.html?stream=top

[15] Consider also: in their recent letter to Transportation Secretary Chao, Senators Cornyn and Baldwin underscore and detail the threat posed to the United States by Chinese buses (in addition to railcars). https://www.documentcloud.org/documents/6781588-Cornyn-Baldwin-TIVSA-Implementation.html

[16] See my 2019 testimony for allegations to this effect raised by U.S. officials in 2017. An additional concern, more generally, is the potential for data manipulation. In the financial services sector, for instance, transactions take place in milliseconds. The ability to slow the transmission of signals could allow a malicious actor to attain control or dominance of the market. Eftimiades interview (February 18, 2020).

The transportation sector as a whole also intersects with and supports other critical U.S. sectors and national functions. Notably, U.S. national defense is to an extent dependent upon the integrity of the transportation sector. If compromised, the ability of U.S. forces to deploy, project power, and achieve their goals and objectives (collectively known as Mission Assurance), may be placed into jeopardy.[17] Consider the potential for cyber/physical convergence, with concomitant consequences on the battlefield.

Widening the aperture further, foreign State-owned enterprises and the advanced technologies that they offer, at relatively low cost and often with concessionary financing, pose a dilemma for other critical infrastructure sectors as well. Case in point: 5G telecommunications technology from Chinese companies Huawei and ZTE.

5G is the bedrock for next-generation networks worldwide. The strategic significance of 5G is reflected in the Prague Proposals, recognized by more than 30 countries worldwide.[18] Who builds and contributes to these networks matters deeply, and each country's decision on the matter will affect not only their telecommunications sector but also every other sector and function that depends on telecommunications (such as transportation, including autonomous vehicles).

Huawei and ZTE are competing aggressively to serve as suppliers worldwide; but America is rightfully taking a hard line at home and urging allies to do the same, based on evidence of these two companies' complicity with the Chinese government. Just last month, the U.S. Department of Justice revealed new charges against Huawei, citing racketeering and conspiracy to steal trade secrets.[19]

Other products and technologies supplied by Chinese companies that have raised security concerns in the United States include video surveillance equipment manufactured by Hangzhou Hikvision Digital Technology and used in U.S. schools and other sensitive (military/diplomatic) sites. At inception, Hikvision was a Chinese government research institute. State-owned enterprises retain a 40-plus percent stake in the company.

Many other smaller but still important opportunities exist for foreign State-owned enterprises to make inroads into U.S. critical infrastructure sectors either directly or indirectly. Flush with State support, these foreign enterprises can buy up U.S. assets/entities that are on the verge of bankruptcy or in need of start-up funding. Such acquisitions may relate only to a component, such as switches; but switches are key to the safe operation of passenger and freight rail.

---

[17] Auburn University Center for Cyber and Homeland Security, *Strengthening Defense Mission Assurance Against Emerging Threats* (May 2019), http://cchs.auburn.edu/_files/mission-assurance-policy-forum-summary.pdf

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

[19] "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," (February 13, 2020), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering

In the context of rail transit systems, switches and precision timing go hand-in-hand. The wider trio of issues — positioning, navigation, and timing (PNT) — also merits a quick sidebar: China is investing heavily to safeguard its own PNT functions and undermine those of others (including through anti-satellite capabilities that could blind and bind the U.S. military, which relies heavily on space-based assets for transit and targeting requirements and other needs).[20]

Whether in relation to the transportation sector or beyond, supply chain and concomitant counterintelligence and national security concerns are certainly not limited to Chinese-origin goods and services. Russian anti-virus software produced by Kaspersky Lab, for example, poses similar concerns and for this reason is subject to a ban on use by U.S. federal agencies.

A final word on threat: the Internet of Things raises further the salience of the concerns expressed here as it continues to expand the potential surface of attack; think sensors, smart cities, and smart cars. While it may not be possible to eliminate all vectors of attack, it is imperative that we seek to limit them and at the same time, cultivate resilience — the ability to minimize the impact of, and bounce back from, an incident.

Selected Policy Recommendations

Turning to counter-threat measures, I would be remiss if I did not begin by giving credit where it is due. A solid step in the right direction is S. 846, the Transit Infrastructure Vehicle Security Act. This legislation, co-sponsored by Chairman Crapo and Ranking Member Brown (plus others including Senators Shelby and Jones), represents precisely the sort of precautionary action needed.[21]

With its incorporation into law as part of the National Defense Authorization Act (NDAA) for Fiscal Year 2020, new public transit system railcars will be subject to cybersecurity certification; a specific category of countries of concern will be barred from participating in rolling stock procurement bids solicited by public transit systems; and the "next-generation" buildout of the National Capital's rail transit system (Metrorail's 8,000-series cars) will be insulated from penetration by CRRC.[22]

---

[20] The new Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services issued on February 12, 2020, is a welcome development. https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/

[21] S. 846 is the basis of language that was ultimately enacted into law in Section 7613 of the National Defense Authorization Act for Fiscal Year 2020 (P.L. 116-92).

[22] The Washington Metropolitan Transit Authority is poised to contract for its "next-generation" rail cars; the deal could be worth over $1 billion. Justin George, " Metro's next-generation rail cars will not be made in China," *Washington Post* (January 25, 2020), https://www.washingtonpost.com/local/trafficandcommuting/metros-next-generation-rail-cars-will-not-be-made-in-china/2020/01/25/1d848c7e-3e06-11ea-baca-eb7ace0a3455_story.html. For a helpful (plain-language) elaboration of some of the key implications of the relevant NDAA provision, see: Bethany Allen-Ebrahimian, "Senators warn of threats posed by Chinese rail companies," *Axios* (February 20, 2020), https://www.axios.com/china-rail-car-threat-senators-transportation-beb72eaf-9c25-4dc0-a88a-f42d2a37d793.html

The provision (NDAA Section 7613) that speaks to cybersecurity certification underscores the importance of "third-party testing and analysis" in addition to "voluntary standards and best practices" developed under the aegis of the National Institute of Standards and Technology (NIST) and the Secretary of Homeland Security. This is a prudent and laudable approach. Certifications, underpinned by common standards and third-party testing, has proven successful in moving markets in other industries. In fact, I would go a step further and suggest that the general principles of the cited provision (Section 7613) should apply also to other critical infrastructure sectors.

In charting a course forward, the challenge is to maintain and enhance U.S. national security while limiting collateral damage to other U.S. interests. Put starkly, we must figure out a way to preserve and advance our security without undermining unduly the U.S. economy. While this need not be an either/or proposition, the way forward will require sustained leadership and determination on the part of both government and industry, coupled with a willingness and ability to prioritize. More fundamentally, it may require us to look deeper at how to better leverage market forces to incentivize security. This may mean creating a greater demand for security from consumers in the products and services they buy. It may also mean incentivizing suppliers to prioritize security as a differentiator in the products they produce. Action will entail costs; but inaction will ultimately be far costlier.

In practice, therefore, we should begin with the Lifeline Sectors, which are the most critical of the critical. These include the defense industrial base, energy (electricity, oil, natural gas), financial services, transportation, telecommunications, and water. Together with the list of National Critical Functions identified by the National Risk Management Center, is a good place to start in terms of prioritizing our efforts to elevate and monitor security concerns, test our response and mitigation measures, and continually refine these regimes. All risk management proceeds in cycles, and national risk management is no exception. Risk identification, assessment, and management must be continuous, adaptive, and forward-looking. A reactive or regulatory "check-the-box" approach simply will not do.

Part of this exercise must involve scrutinizing supply chains. While helpful steps have already been taken — such as Executive Order 13806 on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States[23]; and the Information and Communications Technology Supply Chain Risk Management Task Force launched by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) — efforts must be widened and deepened.[24]

---

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

[24] Robert Kolasky, Director, National Risk Management Center (CISA, DHS): 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://www.congress.gov/116/meeting/house/108931/witnesses/HHRG-116-HM07-Wstate-KolaskyB-20190226.pdf at page 5. See also, DHS CISA et al., *Internet of Things Security Acquisition Guidance - Information Technology Sector* (February 2020), https://www.cisa.gov/sites/default/files/publications/20_0204_cisa_sed_internet_of_things_acquisition_guidance_final_508_0.pdf.

A "system of systems" approach is also needed on the technology side in order to properly integrate advancements into the broader ecosystem. To date, we have fallen short on this count. As remedy, an R&D effort is needed — in the form of a nationwide network of technology testbeds that simulate a realistic pan-sectoral environment. 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.

A strategic approach is equally needed in terms of integrating cyber factors into our thinking and practices more generally, from the get-go, rather than retrofitting cyber fixes later on when damage is already done. By way of example, risk assessments and risk management strategies should not be treated as a separate vertical; instead, they should be integrated from inception. Along similar lines, a domestic version of The Prague Proposals[25] could prove useful for safeguarding U.S. Lifeline Sectors and National Critical Functions in relation to the rollout and widespread implementation of 5G technology. Ultimately, the United States must continuously identify the industries and technologies critical to national and economic security and take steps to reduce vulnerability at both a macroeconomic and microeconomic level.

In furtherance of much of the above (and to inform cyber policy and programs more generally), it would be helpful to have in place a dedicated and official entity that is tasked with collecting and providing data (statistics) on cybersecurity and the broader cyber ecosystem. Both the government and the private sector lack reliable, comprehensive, and empirical metrics on which to base public policy and risk management practices, respectively. We must seek to apply the same level of rigor, clarity, and statistical analysis to cybersecurity that we have given to public health, the economy, and criminal justice.

In addition, resources — both human and capital — are needed. To this end, building the nation's cyber workforce should be a national imperative and addressed urgently, as there is a disturbing deficit of knowledge and bandwidth in our public institutions and in our companies in relation to countering and thwarting cyber threats posed by State actors to U.S. critical infrastructure.

Regarding the machinery of government: in order to properly safeguard U.S. national and economic security in this context, the arms and legs of the U.S. government will have to recalibrate their efforts and synchronize them ever more intensely to better support top-priority critical infrastructure and nation critical functions. For example, the FBI is already working to lash up and grow its Cyber and Counterintelligence Divisions, in order to counter advanced and persistent adversary activity. This is a solid start, but must be continued, enhanced, and expanded over time. Another important partner in the mission is the National Security Agency and in particular its Cybersecurity Directorate. That entity's role in fusing foreign intelligence and cyber defense will be instrumental to Department of Defense Mission Assurance (among other things).

[25] These principles regarding the "cyber security of communication networks in a globally digitized world" were generated at the 5G Security Conference (2019) in which 32 countries participated. *Supra.*

Finally, I would like to add that the U.S. Cyberspace Solarium Commission, of which I am a member, took on many the above-discussed issues throughout the course of our work. Our forthcoming report, due out on March 11th of this year, lays a clear path forward to increase the effectiveness of U.S. government collaboration, resilience of critical infrastructure, security of the cyber ecosystem, and public-private partnership.[26] I look forward to continuing the conversation, and to working further with you and your colleagues in the weeks ahead, on these matters of national importance.

Conclusion

Thank you for the opportunity to testify before you today.[27] I look forward to trying to answer any questions that you may have.

[26] The Commission worked across industry, academia, the Congress, and the executive branch to arrive at workable solutions to strengthen the security posture of the United States in cyberspace. Our forthcoming report organizes nearly 80 recommendations across six pillars**.**

[27] Thank you also to my Deputy Director, Sharon Cardash (with Auburn's Center for Cyber and Homeland Security), for her skillful assistance in preparing this testimony.