U.S. Freight Rail & Transit Cyber Vulnerabilities

Updated July 16, 2019

Table of Contents

1. Executive Summary 1
2. Introduction 2
3. China's Global Rail Ambitions 3
4. China's U.S. Transit & Freight Rail Ambitions 4
5. Current National Security Threats to U.S. Metro and Passenger Rail Systems 4
6. Recent Examples: China the Aggressor 5
7. Future National Security Threats to U.S. Freight Rail 6
8. What Lies Ahead? 7
9. Conclusion 9
10. Citations 10

The Veretus Group is a Washington-based investigative and intelligence firm that provides clients with high quality, actionable information to help facilitate their most important decisions and address their most complex problems.

We are headquartered in Washington, DC, with an office in London, giving us a central platform to assist clients in the U.S. and around the world. Our professionals have extensive experience with intelligence and national security matters and have lived and worked in over a dozen countries and maintain networks of contacts and trusted firms worldwide.

VERETUS GROUP

1. Executive Summary

Consideration of the cyber threats to rail transportation must be an integral part of decision-making by all affected parties: companies, shippers, operators, transit authorities, regulators, and the like. While economics will play an important part of that process, the default position should be protecting the supply chain, operations, and communications platforms from any potential or inherent vulnerabilities. This paper focuses on the cyber threat that market entry and interest to dominate that system by a Chinese state-owned enterprise ("SOE") poses to our U.S. public rail transportation and private sector freight rail systems.

The threat from all malevolent actors is real and increasing; the threat from one state actor—China—presents the largest challenge but one that must be addressed in a head-on fashion and adhered to with a consistent message. CRRC, a Chinese SOE following the dictate of the party-state as expressed in "Made In China 2025," seeks to dominate the global rail equipment market and has targeted the U.S. transit railcar industry as a priority objective: first Boston, then Chicago, Los Angeles, and Philadelphia. With their sights set on Washington, DC and New York, are their motives purely economic, or is there an element of cyber access in their strategy? Our U.S. freight rail infrastructure is also at risk from a concerted effort by Chinese hackers, several examples of which are described herein.

Our most serious adversaries think strategically and long-term. They are patient and willing to take incremental victories on their way to achieving strategic goals such as market domination, access to systems for cyber exploitation, and preparing the battlespace for active measures (covert action). From both an industry standpoint and to protect national security equities, concrete steps should be taken to ensure system integrity, strong cyber defense, and a robust, healthy domestic manufacturing base. We should build on the solid foundation established by the Association of American Railroads ("AAR") as a central point for coordinating cybersecurity efforts, as well as the AAR leadership role in cyber threat information sharing across the industry.

2. Introduction

Our nation's critical infrastructure is under constant threat from malevolent actors — nation-states, international criminal enterprises, issue-driven individuals, and terrorist groups — with cyber being the most common attack vector. The robust network that supports the bulk of the U.S. economy is transportation, of which public transportation and freight rail constitute increasingly important components. As we move toward a more interconnected and automated world, rail will rely more and more on wireless sensor technology, wireless communications devices, the industry's train control systems, product/commodity monitoring, advanced signaling systems for at-grade highway/rail crossings and other hardware and software products, thus increasing the number of potential entry points for hostile actors. To ensure the safety of our rail infrastructure, industry, regulators, oversight organizations (such as the Committee on Foreign Investment in the United States), Congress and the Administration—working closely with industry and the well-considered standards for freight rail Class 1 traffic by the Association of American Railroads ("AAR")—must integrate effective cyber security protocols into the decision-making processes for procurement, system maintenance, and operations.

State actors possess the most sophisticated tools[i] available to survey, map, analyze, and develop software designed to aid continued collection or exploitation of any train management system. Once vulnerabilities in a system are identified, additional tools can be developed and kept at the ready to degrade, alter or destroy data and control systems. Russia, Iran, and North Korea, for example, enjoy extensive capabilities and capacity to conduct offensive cyber operations that exploit their targets and promote their interests—interests that are often inimical to those of the United States and our allies. China, on the other hand, not only is a significant supplier of rail equipment to the U.S., they have demonstrated time and again that they will take advantage of access to systems to collect protected intellectual property and take any steps necessary to secure market domination. Chinese efforts have included cyber-attacks against the U.S. defense, pharmaceutical, and telecommunications industries. A recent insider attack perpetrated by a Chinese national against a locomotive manufacturer in Chicago makes clear that the U.S. rail industry is also becoming a target.

China's provision of commuter and transit railcars and other hardware, much of it interconnected within the cybersphere, combined with their clear intention to expand market position in the U.S. freight rail supply chain puts their SOEs, and by extension the Chinese government, in a position to collect information about our national transportation infrastructure and exploit access to develop tools that could be used against the U.S. economy, coopt personal privacy or degrade our military capabilities in the event of actual hostilities. Our rail systems, particularly freight, are moving toward more automation, more integrated feedback and control systems, and a ubiquitous system of sensor technology. Given current and future unconsidered or even unimpeded Chinese access to the U.S. rail system, ignoring the economic, espionage, active measures, and military threats Chinese SOEs present to critical rail infrastructure would be folly, and one for which we eventually could pay a heavy price should the Chinese government ever get a "God's eye view" of our entire freight network.

[i] "Tools" is a generic term for strings of code designed for exploitation (collection enabling analysis) or attack. Code that is designed to destroy data or infrastructure, for example, could also be described as a cyber weapon.

3. China's Global Rail Ambitions

China has utilized its SOE CRRC Group to further the country's global ambitions.[ii] CRRC's rolling stock manufacturer (CRRC Corp. Ltd.) was founded in 2015 through the merger of China's two biggest train manufacturers. It controls more than 90% of the Chinese railway market, which is the world's largest.[1] It advertises itself as the world's largest supplier of rail transit equipment, and it has posted on social media about its desire to fully "conquer" the rest of the market.[2] CRRC's global ambition fits neatly within China's broader international geo-political aims. China's "Made in China 2025" economic plan (which debuted in May 2015) makes clear that it is seeking a competitive advantage in the global rail transportation sector.[3] CRRC, with its deep ties to the Communist Party of China, largely carries out this initiative in the global rail sector.[4] CRRC is also a key feature of China's "One Belt, One Road" foreign policy and economic expansion initiative. The program aims to build regional and global trade routes through Chinese-financed infrastructure projects, including key strategic sites in the rail sector.[5]

CRRC can, in time, dominate world rail markets by utilizing the support it receives from the Chinese government to drastically underbid otherwise competitive global suppliers.[6] CRRC has received billions of dollars in subsidies, state financing, and other resources from the Chinese government.[7] CRRC's history in Australia paints a bleak picture of the impact a state-sponsored supplier in the rail industry can have on a nation's rail supply chain. In 2008, CRRC comprised around 40% of rail-related demand in Australia; by 2016 it supplied more than 95% of the Australian demand.[8] It took less than a decade for CRRC to leverage underpricing and anti-competitive behavior to collapse Australia's domestic freight rail manufacturing industry.[9] In doing so, China is able to functionally eliminate the market possibility for the trusted and secure development, much less the market viability, of numerous rail technologies. Killing off competition and becoming a "single source" provider also impedes innovation.

China has also specifically sought to advance its domestic capabilities in developing the next generation of rail technologies. China has its own implementation of an automated train control system, analogous to Positive Train Control ("PTC"),[iii] known as the Chinese Train Control System ("CTCS"). It is developing a new generation of this technology that incorporates artificial intelligence ("AI").[10] In 2017, CRRC subsidiary CRRC Zhuzhou Locomotive received ¥10 million ($1.5 million) in Chinese Government subsidies to digitize its rail traction system. The next year, it received an additional ¥9 million ($1.3 million) in Chinese Government subsidies for developing an autonomous driving system project, among other projects.[11]

[ii] CRRC Corp. Ltd. is publicly traded on The Stock Exchange of Hong Kong (1766.HK) but its parent company CRRC Group Corporation is a Chinese state-owned holding company; *Reuters*, "CRRC Corp Ltd (1766.HK)", https://www.reuters.com/finance/stocks/overview/1766.HK; *Sovereign Wealth Fund Institute*, "List of State Owned Enterprise Profiles in Asia", https://www.swfinstitute.org/profiles/state-owned-enterprise/asia.

[iii] Positive Train Control ("PTC") systems are technologies designed to automatically stop a train before certain accidents related to human error occur; *Association of American Railroads*, "Freight Railroads & Positive Train Control", https://www.aar.org/campaigns/ptc/.

4. China's U.S. Transit & Freight Rail Ambitions

CRRC established its first regional beachhead in the U.S. in 2016.[12] The company's executives have been clear in repeatedly stating that the U.S. is a key market for CRRC. For instance, CRRC Qingdao Sifang's vice president Li Yongle told the *Chicago Tribune* in March 2017 that the U.S. was an "important and strategic market" for the SOE.[13]

Since entering the U.S. market, CRRC has secured passenger railcar contracts in Los Angeles, Chicago, Boston and Philadelphia.[14] In pursuing transit rail contracts in the U.S., CRRC has regularly submitted bids that are 20% less than its competitors'. In one instance, the Chinese bid was half as much as that of another competitor.[15] Beyond securing contracts, CRRC is establishing production and assembly facilities in the U.S.; it broke ground on one in Springfield, Massachusetts in September 2015, and another in Chicago, Illinois in April 2017. It is in the process of building a third assembly plant in Los Angeles, California.[16]

While CRRC has thus far focused on the U.S. passenger railcar business, it has begun to use this as a foothold to target our domestic freight rail market. In May 2018, CRRC restructured its freight rail supply business under the name CRRC Qiqihar Group Co. Ltd. The company announced at the time that its freight car business served 54 countries including the U.S.[17] This is in line with CRRC's stated goal to take overseas sales from 7% of its overall transactions in 2015 to 35% by 2025.[18]

5. Current National Security Threats to U.S. Metro and Passenger Rail Systems

Becoming reliant on SOEs such as CRRC imperils our national security by forcing dependence on a foreign power for critical infrastructure. Even if SOEs like CRRC were not able to dominate the domestic American supply chain (as done in Australia), market penetration into the U.S. public transportation railcar sector by a nation state poses a threat to our national security.

In April 2019, a number of U.S. Senators raised concerns about a CRRC bid to supply passenger rail cars to the Washington, D.C. Metropolitan Area Transit Authority because of its impact on U.S. national security.[19] Similarly, in May 2019, a bipartisan group of Members of the U.S. House of Representatives raised the same inherent concerns about a CRRC bid for New York's Metropolitan Transit Authority.[20] SOEs can use supplied passenger railcars and their associated technologies to collect intelligence about passengers. For example, commuter trains manufactured by CRRC contain Wi-Fi systems, automated train control systems, automated passenger counters, and surveillance cameras that could be leveraged for espionage, personal privacy invasion, or sabotage.[21]

Additionally, cooperation between North Korea, Russia and Iran and China should not be ignored. As we provide our close allies with access to certain systems and capabilities, there are several examples of these key adversaries cooperating to oppose the interests of the U.S. Let's take Iran, for example. Should our disputes with Iran become even more hostile, many analysts believe Iran will pursue asymmetric attacks on our financial, communications, and transportation

facilities.[22] Iran has its own cyber forces but its access to and ability to affect these systems would be greatly expanded through cooperation with the Chinese.[23] Given the difficult nature of attribution in the cyber domain, if China assessed there would be little downside to assisting Iran, they would probably do so as long as such cooperation did not significantly affect their national economy in the long run.[24]

6. Recent Examples: China the Aggressor

China has and will continue exploiting cybersecurity vulnerabilities in the U.S. for its strategic advantage. The Chinese have devoted significant resources to the endeavor and have developed offensive cyber-espionage units.[25] Public reporting in the wake of attacks makes clear that the Chinese government is motivated and capable:

- Between 2009 and 2013, Canadian permanent resident and Chinese national Su Bin hacked into the computer systems of large U.S. defense contractors like Boeing to steal data on military projects. With the help of two unnamed Chinese hackers, Su targeted fighter jets such as the F-22 and F-35, as well as the C-17 cargo plane program. He then attempted to sell the information to Chinese SEOs.[26]

- In 2014, hackers connected to China breached the U.S. Office of Personnel Management's ("OPM") servers. The servers contained roughly 18 million copies of the detailed questionnaire completed by individuals seeking a federal security clearance. The questionnaire mandates that candidates answer probing questions about their finances, relationships, health, and any possible substance abuse history. The infiltrators also gained access to the complete personnel files of 4.2 million government employees.[27]

- In December 2018, the U.S. Department of Justice ("DOJ") indicted two Chinese nationals, Zhu Hua and Zhang Shilong, on charges of conspiracy to breach computer systems, wire fraud, and identity theft. The two Chinese nationals had ties to China's Ministry of State Security ("MSS"), China's foreign intelligence service. They targeted U.S. aviation, telecommunications, pharmaceutical, and satellite companies. They also sought to breach governmental bodies including the U.S. Navy, as well as NASA's Goddard Space Flight Center and its Jet Propulsion Laboratory ("JPL").[28]

More broadly, in the last two years we have seen heightened concern regarding China's use of technology platforms to infiltrate systems and networks and establish "back doors" for siphoning information back to China. Examples include the US government restrictions on made-in-China DJI drones, that were culpable for back-channeling imagery and information on US areas of interest back to China, detailed in classified studies.[29] Further, a recent Executive Order effectively bans any US company from using equipment from Huawei, not based on trade tariffs, but on similar national security concerns of Chinese government spying.[30] In the hardware supply chain of chips for Amazon and Apple, it is alleged that China slipped pencil tip–size spy chips into a hardware supplier, Super Micro, which itself relied on subcontractors in China.[31]

A recently publicized indictment of a Chinese national for nine counts of theft of trade secrets from a U.S. locomotive company makes clear the U.S. rail industry is becoming a target. On July 11, 2019, the DOJ unsealed a December 2017 indictment against Xudong "William" Yao, a former employee of a Chicago-based locomotive manufacturer. Yao stole more than 3,000 unique electronic files containing trade secrets relating to the systems that operate the manufacturer's locomotives. The proprietary information included the firm's software source code and technical documents. Yao then transported copies of the files and documentation to China, where he began working for a manufacturer of automotive telematics service systems.[32] At the time of writing, Yao is on the U.S. Federal Bureau of Investigation's "Most Wanted" list and is believed to be living in China.[33]

7. Future National Security Threats to U.S. Freight Rail

The next generation of rail infrastructure projects will increase the safety, reliability, and efficiency of the U.S. freight rail network, but also presents new cybersecurity risks. Accelerating technologies include the implementation of advanced signal and train control systems, increased incorporation of various sensors and onboard communications platforms, and new connections to networks with internet exposure. Initial PTC technology in the U.S. is deployed as a safety overlay system and, as configured, does not lend itself to malicious exploitation. Following the full implementation of the present version in 2020, however, the layering of additional capabilities towards a vision of enhanced rail automation will present new vulnerabilities.

The technologies involved in the next generation of rail projects (including satellite, cellular, and radio communication) are complex and carry pre-existing vulnerabilities that are likely to be exploited in the rail sector.[34] There is the conventional need to provide cybersecurity protection to information technology ("IT") systems, networks, and data — and the technologies that combine IT and operational technology ("OT") — known as the expanding world of the Internet-of-Things ("IoT"). IoT devices are a convergence of mobile computing, embedded systems, and remote access for monitoring, trouble shooting, and reconfiguration of a physical device through wireless communications, elements of data capabilities (processing and storage) and transducer capabilities (sensing and actuating). IoT sensors in public environments can contribute to the aggregation and analysis of vast amounts of data about both infrastructure and individuals; IoT devices with actuators can make changes to physical systems, and if compromised could allow an adversary to cause disruptions, endanger human safety, and damage or destroy facilities and equipment. Protecting the provenance of software, networks, and components of IoT is paramount in risk mitigation.

With the introduction of these technologies, risk becomes linear in that the adoption of each additional connected wireless sensor and command technology is a new attack target for malicious actors.[35] This linear risk is compounded by the real-time and time-sensitive nature of the information involved. In critical systems with safety expectations that require minimizing downtime, traditional cyber-defense technologies (i.e. firewalls, whitelisting, etc.) may inject delays that could unintentionally disrupt integrated rail system network functions.[36] Given the long design life of the highly reliable systems used in freight rail, it is especially important that the foundation for technological advancements is secure. Failure to ensure a secure foundation could

result in compounding vulnerabilities as legacy systems face requirements to interact with newly developed technologies.[37]

Beyond risks involved with the implementation of new rail technologies, the sourcing of critical components presents possibly more significant opportunities for adversaries. As technology progresses, the supply chain for sourcing and maintaining new technological assets in freight rail becomes increasingly complex, giving adversaries additional opportunities to corrupt or sabotage infrastructure through infiltration.[38] Recognizing severe vulnerabilities in the electronic components and software supply chain, the U.S. Department of Defense ("DOD") recently formed a strategy for supply chain security and resilience, labeled "Deliver Uncompromised." Elements of the strategy include continuous monitoring of software, supply security in contracts, and expanding DOD authority to "never contract with the enemy."[39] This initiative extends beyond DOD to all the departments of government.

8. What Lies Ahead?

Previous attacks on U.S. public transportation and freight rail infrastructure provide clear and convincing evidence that our adversaries intend to cause harm; however, the scope and depth of that harm has yet to be determined. But if history is a guide, the August 2003 attack on CSX Corporation's freight rail service by the "Blaster" computer worm that caused cancellations and delays is informative.[40] Metropolitan rail systems in California (San Francisco and Sacramento) were both hit by separate ransomware attacks in 2017.[41] In February 2018, Colorado's Department of Transportation suffered a ransomware attack that reduced its employees to using pen, paper, and their personal devices to maintain operations.[42] While each attack impacted a transportation agency or a rail line's operations, the impacts were structurally limited to that organization's IT and administrative systems, as those were the only network-connected resources. With implementation of the next generation of rail technologies, *this limitation will no longer exist in public transportation or freight rail*.[43]

Other attacks have surely been avoided thanks to the U.S. rail industry's efforts to protect digital infrastructure. For example, the Association of American Railroads ("AAR") assembled the Rail Information Security Committee ("RISC") in 1999 to serve as a central body for coordinating cybersecurity efforts.[44] Industry efforts were expanded after the September 11, 2001 terrorist attacks on the U.S. Today, the industry works closely with its partners at the U.S. Department of Homeland Security, the U.S. Transportation Security Administration, Transport Canada, and the Federal Bureau of Investigation.[45]

Information sharing and integrated planning are now a norm within the U.S. Rail industry, ensuring that U.S. rail stays ahead of threats.[46] AAR also independently maintains a Cyber and Security Working Committee within its Policy and Advocacy Management Committee to study and recommend best practices in the industry. The railroad companies have also integrated internal cybersecurity norms into procurement to ensure that newly purchased technologies meet security standards.[47]

Attacks on next-generation railroad technologies could take many forms, such as passive eavesdropping, whereby the attacker surreptitiously gathers information; active denial of critical

train controls, in which the system is functionally jammed to prevent commands from being carried out; and/or active assumption of control, where an attacker gains controls over the system itself.[48]

In assessing the possible consequences of cyber-attacks on upcoming rail technologies, it is useful to examine attacks on other industries' industrial control systems ("ICS").[iv] Cybersecurity experts have seen an increase in malicious cyber activity targeting ICS, with dedicated nation-state affiliated groups engaging in intrusion of ICS to perform reconnaissance for possible future exploitation.[49] The next-generation systems being implemented all depend upon ICS, which creates new avenues for utilizing previously developed ICS attacks on compromised rail infrastructure.[50] Chinese SOEs entering the U.S. freight network through the sector's supply chain would provide China's intelligence and espionage apparatus a direct avenue for effectuating these threats.

SOEs could use their entry into the next-generation rail supply chain to collect intelligence about the movement of freight across our rail network, including the locations of hazardous material freight shipments sitting in or passing through major metropolitan cities.[51] This could give adversaries early and reliable warnings with a "God's eye view" of U.S. preparations for conflict, as the rail network is a vital part of U.S. military logistics. In this scenario, even limited infiltration of the railways in civilian sectors could allow adversaries to discern patterns in traffic. As rail carries roughly 40% of freight by ton-miles,[v] the intelligence collected by an adversary could be used to detect shortages in strategically important sectors for subsequent economic exploitation.[52]

Disruptions in freight rail systems caused by future cyber-attacks could have significant consequences. A single successful attack leveraging an SOE's components could re-position a switch from a mainline onto an occupied siding, making a collision, and the possible loss of human life, all but certain.[53] An attack could facilitate unauthorized hardware commands that result in environmental damage.[54] Adversaries could also create misinformation such as false sensor readings that could obscure or otherwise allow the undetected release of hazardous materials in highly populated areas.[55]

For the rail industry itself, the potential consequences of a cyber-attack are numerous, including: financial losses, compromised operations, theft of data, liabilities relating to the safety of personnel and the public at large, and reputational damage. The average financial cost of a cybercrime incident (regardless of industry) is $13 million.[56] Beyond the direct consequences of an attack, the post attack remediation and recovery can be economically and operationally substantial, with long lasting implications. It took the City of Atlanta's Department of Transportation months to recover from a March 2018 ransomware attack.[57] In the transportation sector, shipping company A.P. Møller – Mærsk A/S spent up to $300 million in recovery costs after a 2017 ransomware attack that disrupted operations at terminals for weeks.[58]

[iv] Industrial control systems ("ICS") describes the different types of control systems and associated instrumentation used to operate and/or automate industrial processes. *See Trend Micro*, "Industrial Control System," https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system.

[v] Ton-miles is defined as one ton of freight hauled one mile.

9. Conclusion

It is paramount that we focus on emerging cybersecurity risks given the strategic importance of the security of U.S. freight rail, passenger rail, and metro rail systems to our economy and national interest. As the industry works to implement technological advancements that improve safety, reliability, and efficiency, the emphasis must be on ensuring that technological improvements are made so as to preserve the integrity of U.S. rail systems and by extension U.S. interests. These objectives can only be accomplished through diligent efforts strengthening industry and government cooperation.

10. Citations

[1] *China Business Review*, "Merger of China's Two Largest Rail Companies Forms $26 Billion Firm", published January 14, 2015, https://www.chinabusinessreview.com/merger-of-chinas-two-largest-rail-companies-forms-26-billion-firm/.
[2] *CRRC Corporation Limited*, "About Us", https://www.crrcgc.cc/g5141.aspx; Tweet by CRRC Corporation Ltd (@CRRC_global), https://admin.govexec.com/media/gbc/docs/pdfs_edit/crrc_global_market%5B3%5D.jpg.
[3] *The Washington Post*, "Could a Chinese-made Metro car spy on us? Many experts say yes.", published January 7, 2019, https://www.washingtonpost.com/local/trafficandcommuting/could-a-chinese-made-metro-car-spy-on-us-many-experts-say-yes/2019/01/07/00304b2c-03c9-11e9-b5df-5d3874f1ac36_story.html?utm_term=.97f5afd6d625.
[4] *Brigadier General John Adams (Ret.)*, "National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector – Threats and Mitigation", published October 22, 2018, http://railsecurity.org/wp-content/uploads/2018/10/RSA-National-Security-Risks-to-US-Freight-Rail-Report-Final.pdf; *The Epoch Times*, "US Experts, Lawmakers Highlight China's Threat to US Rail Security", published April 3, 2019, https://web.archive.org/web/20190404133504/https://www.theepochtimes.com/us-experts-lawmakers-highlight-chinas-threat-to-us-rail-security_2865033.html.
[5] *Executive Interagency Task Force in Fulfillment of Executive Order 13806 (US Department of Defense),* "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States", published 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.
[6] *Eno Center for Transportation*, "China Transit Procurement Ban Has Potential to Divide Stakeholders", published May 28, 2018, https://www.enotrans.org/article/china-transit-procurement-ban-has-potential-to-divide-stakeholders/; *The Washington Post,* "China's state-owned rail-car builder looks close to bidding on Metro contract; also eyeing N.Y. subway work", published February 11, 2019, https://www.washingtonpost.com/local/trafficandcommuting/chinas-state-owned-rail-car-builder-looks-close-to-bidding-on-metro-contract-also-eyeing-ny-subway-work/2019/02/11/77c6da4c-2a53-11e9-984d-9b8fba003e81_story.html?utm_term=.00915b39c220.
[7] *The Epoch Times,* "Chinese Interest in US Rail Threatens National Security, Economy, US Experts Say", published May 19, 2019, https://www.theepochtimes.com/chinese-interest-in-us-rail-threatens-national-security-economy-us-experts-say_2928553.html; *Barron's*, "China Rail CRRC Jumps As Beijing Subsidizes Shareholders In $1.8B Share Sale", published May 29, 2016, https://www.barrons.com/articles/china-rail-crrc-jumps-as-beijing-subsidizes-shareholders-in-1-8b-share-sale-1464577503; *Alliance for American Manufacturing*, "Report: The American Freight Rail Network is Unguarded and At Risk", published October 24, 2018, http://www.americanmanufacturing.org/blog/entry/report-the-american-freight-rail-network-is-ungarded-and-at-risk.
[8] *Testimony to the U.S. House of Representatives' Committee on Transportation and Infrastructure from Oxford Economics,* "The Impact of Foreign State-Owned Enterprises on the U.S. Public Transit and Freight Rail Sectors", published May 16, 2019, https://transportation.house.gov/imo/media/doc/Testimony%20-%20Galloway.pdf.
[9] *Alliance for American Manufacturing,* "China is Aiming to Take Over the U.S. Transit Market. So Far, the Plan is Working.", published May 16, 2019, http://www.americanmanufacturing.org/blog/entry/congress-examines-the-threat-of-chinese-state-owned-enterprises-to-the-u.s.; *Reuters,* "China to bid on D.C. Metro rail deal as national security hawks circle", published on May 9, 2019, https://www.reuters.com/article/us-usa-china-trains-crrc-focus/china-to-bid-on-d-c-metro-rail-deal-as-national-security-hawks-circle-idUSKCN1SF0Y5.
[10] *International Railway Journal*, "China's next-generation signaling system targets automatic operation", published July 16, 2018, https://www.railjournal.com/in_depth/chinas-next-generation-signalling-system-targets-automatic-operation.
[11] *Epoch Times*, "US Experts, Lawmakers Highlight China's Threat to US Rail Security", published April 3, 2019, https://web.archive.org/web/20190404133504/https://www.theepochtimes.com/us-experts-lawmakers-highlight-chinas-threat-to-us-rail-security_2865033.html.
[12] *China Daily,* "CRRC on the fast track for global expansion", published June 8, 2017, http://www.chinadaily.com.cn/business/2017-06/08/content_29661737.htm.
[13] *Chicago Tribune*, "First step to new CTA rail cars: Build the factory in Chicago", published March 16, 2017, https://www.chicagotribune.com/business/ct-cta-new-railcar-plant-0316-biz-20170315-story.html; *Shenzhen Daily,* "CRRC Corp. to win $647m LA metro contract", published March 29, 2017, http://www.szdaily.com/content/2017-

03/29/content_15777938.htm; *CNBC*, "China's state-owned rail manufacturer CRRC wants to be part of Trump's US growth story", published May 9, 2017, https://www.cnbc.com/2017/05/09/china-crrc-chairman-on-us-operations-jobs-and-investments.html.

[14] *Reuters,* "Schumer asks government to probe rail tech from China", published May 19, 2019, https://www.reuters.com/article/us-usa-china-trains-crrc/schumer-asks-government-to-probe-rail-tech-from-china-idUSKCN1SP0TQ.

[15] *Defense One*, "Stop China's Infiltration of US Railroads", published November 26, 2018, https://www.defenseone.com/ideas/2018/11/stop-chinas-infiltration-us-railroads/153025/; *The Philadelphia Inquirer*, "Mass.-based company with Chinese backing beats local group for SEPTA car contract", published March 21, 2017, https://www.inquirer.com/philly/business/transportation/Mass-based-company-with-Chinese-backing-beats-out-local-group-for-SEPTA-car-contract.html.

[16] *American Shipper*, "Chinese rail manufacturer CRRC breaks ground on U.S. plant", published September 4, 2015, https://www.americanshipper.com/news/chinese-rail-manufacturer-crrc-breaks-ground-on-us-plant?autonumber=61397&via=sharecodev1*; CRRC Press Release*, "CRRC plant brings hope to Chicago area", published May 9, 2017, http://www.crrcgc.cc/en/g7389/s14333/t285517.aspx. *The Washington Post*, "Senators to Metro: No more federal funding if you buy Chinese rail cars", published April 13, 2019, https://www.washingtonpost.com/local/trafficandcommuting/senators-to-metro-no-more-federal-funding-if-you-buy-chinese-rail-cars/2019/04/13/99d22b7a-5cab-11e9-9625-01d48d50ef75_story.html?utm_term=.ef932a49ab0b.

[17] CRRC Press Release, "CRRC restructured freight train business and established CRRC Qiche Group Co., Ltd.", published on May 24, 2018, http://www.crrcgc.cc/en/g7389/s14333/t292854.aspx.

[18] China Daily, "On the fast track to expansion", published May 12, 2016, http://www.chinadaily.com.cn/business/2016-12/05/content_27566060.htm.

[19] *The Washington Post*, "Senators to Metro: No more federal funding if you buy Chinese rail cars", published April 13, 2019, https://www.washingtonpost.com/local/trafficandcommuting/senators-to-metro-no-more-federal-funding-if-you-buy-chinese-rail-cars/2019/04/13/99d22b7a-5cab-11e9-9625-01d48d50ef75_story.html?noredirect=on&utm_term=.986e773fb4c7.

[20] *The Hill,* "Lawmakers target Chinese rail cars over security concerns", published June 5, 2019, https://thehill.com/policy/technology/446997-lawmakers-target-chinese-rail-cars-over-security-concerns.

[21] *Defense One*, "Stop China's Infiltration of US Railroads", published November 26, 2018, https://www.defenseone.com/ideas/2018/11/stop-chinas-infiltration-us-railroads/153025/.

[22] *Stratfor*, "How Iran's Cyber Game Plan Reflects Its Asymmetrical War Strategy", published December 18, 2018, https://worldview.stratfor.com/article/how-irans-cyber-game-plan-reflects-its-asymmetrical-war-strategy; *Insurance Journal*, "Iran Hackers Could Be Behind Wave of Cyber Attacks on Infrastructure: FireEye", published January 11, 2019, https://www.insurancejournal.com/news/international/2019/01/11/514571.htm.

[23] *RAND Corporation*, "Iran: A Rising Cyber Power?", published December 16, 2015, https://www.rand.org/blog/2015/12/iran-a-rising-cyber-power.html.

[24] *Symantec Corp.,* "The Cyber Security Whodunnit: Challenges in Attribution of Targeted Attacks", published October 3, 2018, https://www.symantec.com/blogs/expert-perspectives/cyber-security-whodunnit-challenges-attribution-targeted-attacks.

[25] *Council on Foreign Relations*, "PLA Unit 61398", https://www.cfr.org/interactive/cyber-operations/pla-unit-61398; *Reuters*, "U.S. warns of new hacking spree from group linked to China", published October 3, 2018, https://www.reuters.com/article/us-usa-cyber-china/u-s-warns-of-new-hacking-spree-from-group-linked-to-china-idUSKCN1ME01L.

[26] *CBC*, "Su Bin, Chinese man accused by FBI of hacking, in custody in BC", published July 12, 2014, https://www.cbc.ca/news/canada/british-columbia/su-bin-chinese-man-accused-by-fbi-of-hacking-in-custody-in-b-c-1.2705169.

[27] *Wired*, "Inside the Cyberattack That Shocked the US Government", published October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[28] *The New York Times*, "U.S. Accuses Chinese Nationals of Infiltrating Corporate and Government Technology", published December 20, 2018, https://www.nytimes.com/2018/12/20/us/politics/us-and-other-nations-to-announce-china-crackdown.html.

[29] *CNN*, "DHS warns of 'strong concerns' that Chinese-made drones are stealing data", published May 20, 2019, https://www.cnn.com/2019/05/20/politics/dhs-chinese-drone-warning/index.html; *DroneDJ*, "DHS warns that Chinese-made drones, including DJI's, might be stealing sensitive data", published May 20, 2019, https://dronedj.com/2019/05/20/dhs-chinese-made-drones-dji-stealing-data/.

[30] *CNBC*, "China pencil-tip spy chip's ultimate market risk: The profits built on big tech's low-cost global supply chain", published Oct 6, 2018, https://www.cnbc.com/2018/10/05/chinas-cyber-spying-keeps-a-lot-of-us-tech-ceos-up-at-night.html
[31] *Bloomberg Businessweek*, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", published October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
[32] *The United States Department of Justice*, "Newly Unsealed Federal Indictment Charges Software Engineer with Taking Stolen Trade Secrets to China", published July 11, 2019, https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china; *The Washington Post,* "Software engineer accused of taking trade secrets to China", published July 11, 2019, https://www.washingtonpost.com/business/technology/software-engineer-accused-of-taking-trade-secrets-to-china/2019/07/11/23a8a1c2-a3fa-11e9-a767-d7ab84aef3e9_story.html?utm_term=.fa6b974d3897; *Chicago Sun Times*, "Man wanted for taking train manufacturer's trade secrets to China", published July 11, 2019, https://chicago.suntimes.com/2019/7/11/20690604/xudong-william-yao-wanted-theft-trade-secrets-suburban-train-manufacturer-china.
[33] U.S. Federal Bureau of Investigation, "Most Wanted: Xudong Yao," https://www.fbi.gov/wanted/counterintelligence/xudong-yao.
[34] *Railway Technology*, "Will 5G create new cyber threats to global railways?", published June 11, 2019, https://www.railway-technology.com/features/5g-on-railways/.
[35] *Oliver Wyman*, "Cyber Resiliency: A Clear And Urgent Necessity For Modern Railroads", published March 21, 2019, https://www.oliverwyman.com/our-expertise/insights/2019/apr/cyber-resiliency.html.
[36] *American Public Transportation Association*, "Securing Control and Communications Systems in Rail Transit Environments", published June 28, 2013, https://web.archive.org/web/20180425085816/http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-002-13.pdf.
[37] *American Public Transportation Association*, "Securing Control and Communications Systems in Rail Transit Environments", published June 28, 2013, https://web.archive.org/web/20180425085816/http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-002-13.pdf.
[38] *War on the Rocks*, "Cyber Security Derailed? Recommendations for Smarter Investments in Infrastructure", published November 16, 2018, https://warontherocks.com/2018/11/cyber-security-derailed-recommendations-for-smarter-investments-in-infrastructure/.
[39] *Federal News Network*, "DoD thinking of ways to implement 'deliver uncompromised' initiative", April 24, 2019, https://federalnewsnetwork.com/defense-main/2019/04/dod-thinking-of-ways-to-implement-deliver-uncompromised-initiative/.
[40] *Focus on Terrorism* by Edward V. Linden, page 40, published in 2007, https://books.google.com/books?id=wl-Ds42YMDIC&pg=PA40&lpg=PA40&dq=CSX+freight+rail+east+coast+cancellation+delays+%22virus%22&source=bl&ots=dRjmiiIm7g&sig=ACfU3U2b9A36Urb_V3mYZ9M2t3j4D6pAJw&hl=en&sa=X&ved=2ahUKEwjFzcDJ9-biAhVClKwKHehSD6MQ6AEwAXoECAkQAQ#v=onepage&q=CSX%20freight%20rail%20east%20coast%20cancellation%20delays%20%22virus%22&f=false.
[41] *The Verge*, "Hackers are holding San Francisco's light-rail system for ransom", published November 27, 2016, https://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware-cybersecurity-muni; *The Sacramento Bee,* "Hackers attack Sacramento transit system and demand $8,000 ransom", published November 20, 2017, https://www.sacbee.com/news/local/article185669953.html.
[42] *The Pew Charitable Trusts*, "How Hackers Could Cause Chaos on America's Roads and Railways", published April 24, 2018, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/04/24/how-hackers-could-cause-chaos-on-americas-roads-and-railways.
[43] *Automox*, "Poor Cybersecurity: A Threat to the Transportation Industry", published July 27, 2018, https://www.automox.com/blog/poor-cybersecurity-a-threat-to-the-transportation-industry.
[44] *Association of American Railroads*, "Railroads and Cybersecurity", published March 2018, https://www.aar.org/wp-content/uploads/2018/03/AAR-Railroads-Cybersecurity.pdf.
[45] *Association of American Railroads, "Physical & Cybersecurity: Protecting the Nation's Freight Rail Network", https://www.aar.org/article/freight-rail-physical-cybersecurity*.

[46] *Progressive Railroading,* "With rail security planning, information sharing is key", published January 2015, https://www.progressiverailroading.com/rail_industry_trends/article/With-rail-security-planning-information-sharing-is-key--43156.
[47] *Fast Company,* "How railroads are keeping trains safe from hackers", published April 29, 2019, https://www.fastcompany.com/90341548/how-railroads-are-keeping-trains-safe-from-hackers.
[48] *International Conference on Critical Infrastructure Protection,* "Securing Positive Train Control Systems", published in 2007, https://link.springer.com/content/pdf/10.1007%2F978-0-387-75462-8_5.pdf.
[49] *ComputerWeekly*, "Cyber attacks targeting industrial control systems on the rise", published March 27, 2019, https://www.computerweekly.com/news/252460353/Cyber-attacks-targeting-industrial-control-systems-on-the-rise; *ComputerWeekly*, "Industrial control systems a specialised cyber target", published August 7, 2018, https://www.computerweekly.com/news/252446423/Industrial-controls-systems-a-specialised-cyber-target; *Wiley Connected*, "Cyber Attack Highlights Risks to Industrial Control Systems and Potential for Real-World Consequences", published December 19, 2017, https://www.wileyconnect.com/home/2017/12/19/cyber-attack-highlights-risks-to-industrial-control-systems-and-potential-for-real-world-consequences; *AutomationWorld*, "The Infiltration of U.S. Control Systems", published March 28, 2018, https://www.automationworld.com/article/industry-type/all/infiltration-us-control-systems.
[50] *Rockwell Collins*, "The state of cybersecurity in the rail industry", published August 2017, https://www.rockwellcollins.com/-/media/Files/rc2016/marketing/C/Cybersecurity-solutions/The-state-of-cybersecurity-in-the-rail-industry-white-paper.pdf?lastupdate=20171215210046.
[51] *War on the Rocks,* "Cyber Security Derailed? Recommendations for Smarter Investments in Infrastructure", published November 16, 2018, https://warontherocks.com/2018/11/cyber-security-derailed-recommendations-for-smarter-investments-in-infrastructure/.
[52] *U.S. Department of Transportation Federal Railroad Administration*, "Freight Rail Overview", https://www.fra.dot.gov/page/P0362; *U.S. Army*, "Staying on track with military rail", published July 5, 2016, https://www.army.mil/article/169711/staying_on_track_with_military_rail; *Association of American Railroads,* "Railroads & the U.S. Military: Stronger Together", https://www.aar.org/article/freight-rail-military/.
[53] *International Conference on Critical Infrastructure Protection,* "Securing Positive Train Control Systems", published in 2007, https://link.springer.com/content/pdf/10.1007%2F978-0-387-75462-8_5.pdf.
[54] *Rockwell Collins*, "The state of cybersecurity in the rail industry", published August 2017, https://www.rockwellcollins.com/-/media/Files/rc2016/marketing/C/Cybersecurity-solutions/The-state-of-cybersecurity-in-the-rail-industry-white-paper.pdf?lastupdate=20171215210046*; Association of American Railroads, "Freight Rail Hazmat Safety: More than 99.999% of all Tank Cars Reach their Destination Safely", https://www.aar.org/issue/freight-rail-hazmat-safety/*.
[55] *Eno Center for Transportation*, "Chinese State-Owned Enterprises are Eyeing U.S. Freight Rail Manufacturing: Report", published October 22, 2018, https://www.enotrans.org/article/chinese-state-owned-enterprises-are-eyeing-u-s-freight-rail-manufacturing-report/.
[56] *Accenture,* "Ninth Annual Cost of Cybercrime Study", published March 6, 2019, https://www.accenture.com/us-en/insights/security/cost-cybercrime-study.
[57] *The New York Times,* "A Cyberattack Hobbles Atlanta, and Security Experts Shudder", published March 27, 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.
[58] *Oliver Wyman*, "Cyber Resiliency: A Clear And Urgent Necessity For Modern Railroads", published March 21, 2019, https://www.oliverwyman.com/our-expertise/insights/2019/apr/cyber-resiliency.html.