Submitted Statement for the Record of

Kathryn Waldron
Fellow, National Security and Cybersecurity
R Street Institute

Kristen Nyman
Government Affairs Specialist, National Security and Cybersecurity
R Street Institute

Before the

Coast Guard and Maritime Transportation Subcommittee
of the
House Transportation and Infrastructure Committee

Hearing on

China's Maritime Silk Road Initiative: Implications for the Global Maritime Supply Chain

October 17, 2019

Chairman Maloney, Ranking Member Gibbs and Members of the Subcommittee:

Thank you for holding this important hearing on *China's Maritime Silk Road Initiative: Implications for the Global Maritime Supply Chain*. This statement is offered by scholars from the R Street Institute's National Security and Cybersecurity team who have studied supply chain security extensively. The R Street Institute is a nonprofit, nonpartisan public policy research organization whose mission is to engage in research and outreach to promote free markets and limited, effective government.

China's Belt and Road Initiative (BRI) is an ambitious infrastructure development strategy to create a vast global transportation and shipping network aimed at increasing Chinese economic trade. First proposed by President Xi Jinping in 2013, the 21st Century Maritime Silk Road is the sea-based component of this strategy "... designed to extend from China's coast to Europe through the South China Sea and the Indian Ocean in one route, and from China's coast through the South China Sea to the South Pacific in the other."[1] In practical terms, this has led to increased Chinese investment in building and operating ports throughout the world.

While many countries were initially eager to embrace Chinese investment in their infrastructure, concerns over increased public debt have led former partners to shelve development projects.[2] But an inequitable reaping of the economic benefits isn't the only reason some countries are skeptical of the BRI. Indeed, China's development of a modern, maritime silk

[1] National Development and Reform Commission, "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road," Ministry of Foreign Affairs and Ministry of Commerce of the People's Republic of China with State Council authorization, March 28, 2015. http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html.

[2] Amanda Erikson, "Malaysia cancels two big Chinese projects, fearing they will bankrupt the country," *The Washington Post*, Aug. 21, 2018. https://www.washingtonpost.com/world/asia_pacific/malaysia-cancels-two-massive-chinese-projects-fearing-they-will-bankrupt-the-country/2018/08/21/2bd150e0-a515-11e8-b76b-d513a40042f6_story.html; Nyshka Chandran, "Fears of excessive debt drive more countries to cut down their Belt and Road investments," CNBC, Jan. 17, 2019. https://www.cnbc.com/2019/01/18/countries-are-reducing-belt-and-road-investments-over-financing-fears.html.

road also has problematic cybersecurity implications. The two main concerns are supply chain risks for ports that dock U.S. ships and cyber risks that would derive from a Chinese "digital silk road."

Supply Chain Risks for Ports that Dock U.S. Ships

The first concern is that Chinese-built or -operated ports present a national security risk for U.S. or NATO ships docked overseas. Just last year, Shanghai International Port Group, a Chinese company, announced plans to take over management of the Israeli port of Haifa. American stakeholders quickly raised national security concerns over the Chinese-Israeli deal. Former U.S. ambassador to Israel Dan Shapiro stated that "to have a Chinese company operate a port of a close ally potentially poses a significant challenge and maybe a risk for US Navy operations."[3] Retired U.S. admiral Gary Roughead also pointed out that Chinese port management could allow their intelligence agencies to better anticipate U.S. naval activities. But ship movement isn't the only information the Chinese could access: "Significantly, the information systems and new infrastructure integral to the ports and the likelihood of information and electronic surveillance systems jeopardize U.S. information and cybersecurity," Roughhead warned.[4] The potential for hostile foreign governments to access proprietary and sensitive military intelligence is of grave concern to U.S. domestic security, and Congress would do well to address this supply chain vulnerability.

Physical access to ports is not the only maritime supply chain risk involved. China's construction of a "digital silk road" might pose an even greater risk to the U.S. supply chain. Just as the 21st century version of the maritime silk road manifested itself as Chinese investment in

[3] Raphael Ahren, "Has Israel made a huge mistake letting a Chinese firm run part of Haifa port?" *The Times of Israel*, Dec. 20, 2018. https://www.timesofisrael.com/has-israel-make-a-huge-mistake-letting-a-chinese-firm-run-part-of-haifa-port/.

[4] David Brennan, "Chinese Deal to Take Over Key Isreali Port May Threaten U.S. Naval Operations, Critics Say," *Newsweek*, Sept. 14, 2018. https://www.newsweek.com/chinese-deal-take-over-key-israeli-port-may-threaten-us-naval-operations-1121780.

physical infrastructure, the digital silk road would promote Chinese investment in digital infrastructure.

"Digital Silk Road" Supply Chain Concerns

Recent speeches from Xi Jinping and other government officials have pushed Chinese cybersecurity firms to invest in countries where BRI development projects are underway.[5] Their goal, according to Vice-Minister of Information Technology Chen Zhaoxiong, is to build "a community of common destiny in cyberspace."[6] A cyber community of this magnitude fostered by China should raise alarms for anyone in favor of protecting free speech. China's "Great Firewall" reveals the Chinese Communist Party's (CCP) need to maintain operational control of any cyber community.[7] Authoritarian-leaning countries that embrace Chinese investment in their ports, like Malaysia and Vietnam, may also embrace China's exporting of its surveillance technology and policies of authoritarian censorship and Internet control.[8]

Countries more resistant to Chinese-style authoritarianism may also struggle to contain the cybersecurity of their digital ecosystem as Chinese software and hardware becomes more pervasive. The fear that Chinese companies will incorporate backdoors into telecom systems for CCP exploitation has already been a topic of fierce debate thanks to the Huawei situation.

While certain U.S. policymakers may want to bar China from the global digital system entirely, it is simply too late. The digital fabric is too intertwined for any separation to be viable. Unlike the United States, the rest of the world has not shown willingness to ban Chinese companies. Therefore, without allied consensus, we must assume there are no safe systems in cyberspace. Whether a given port is attached to an ocean or a computer, policymakers must keep

[5] Kieran Green, "Securing the Digital Silk Road," Center for Advanced China Research, Feb. 11, 2019. https://www.ccpwatch.org/single-post/2019/02/11/Securing-the-Digital-Silk-Road.

[6] Staff, "China talks of building a 'digital Silk Road,'" *The Economist*, May 31, 2018. https://www.economist.com/china/2018/05/31/china-talks-of-building-a-digital-silk-road.

[7] Bloomberg News, "The Great Firewall of China," *The Washington Post*, Nov. 5, 2018. https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html.

[8] Ralph Jennings, "Chinese Get Chances to Invest in Vietnam Despite Political Rifts," *Voice of America*, Dec. 17, 2018. https://www.voanews.com/east-asia/chinese-get-chances-invest-vietnam-despite-political-rifts.

in mind that China will be keeping a keen eye on everything flowing through it, be it ships or information.

An outright ban-and-sanction plan is infeasible, at least in the long term, in our digitally interconnected reality. The U.S. government does, however, have certain recourses to mitigate supply chain cyber risks.

Policy Recommendations

In order to address maritime supply chain risks, the United States and its allies will have to carefully vet the arrangements they make with regard to port operation and production. The United States should promote economic competition, clearing any trade barriers that impede American companies from bidding on international construction projects. In countries where American companies do not have the capacity to make competitive bids on construction projects, the United States should look for alternative diplomatic opportunities to counterbalance China's political influence and encourage allies to do the same. U.S. policymakers should also continue to point out the strings attached to Chinese investment. Finally, as ports become increasingly automated, the United States should work with international standard-setting organizations and local governments to ensure appropriate cybersecurity controls are built into port cybersystems.

As a prescription for the larger supply chain issue at hand, the government should consider implementing these strategies on a broader scale. Promoting market competition will allow friendlier producers to enter markets currently dominated by Chinese companies. One of the main issues with Huawei, for instance, is that they are one of the only companies on the path to providing 5G.

Another strategy is working with standard-setting organizations, like the International Organization for Standardization, to limit Chinese influence and ensure fair standard-setting, rather than regulations that would benefit any one country's products or production methods.

Collaborating with America's allies to collectively confront bad actors is crucial to ensuring companies with bad practices face enough pressure to change their behavior.

Regardless of the strategic path it chooses, one thing is certain: The United States will have to take decisive action in order to prevent China from gaining outsized influence over the global supply chain and growing from its present nefarious state to an even more dangerous one.

We thank the committee for recognizing the importance of addressing supply chain vulnerabilities. If we can be of any assistance to members of the committee, please feel free to contact us or our colleagues at the R Street Institute.

Kathryn Waldron
Fellow, National Security and Cybersecurity
kwaldron@rstreet.org

Kristen Nyman
Government Affairs Specialist, National Security and Cybersecurity
knyman@rstreet.org