Failed Strategy in Cyberspace

Reliance on foreign supply chains

by Maj Patrick Hylant

>Maj Hylant is an eighteen year Marine Corps Reservist currently assigned MARFORCYBER. His career has been a hybrid mix of civilian and government expertise working Cyber Operations at two prominent Silicon Valley companies and the NSA, USCYBERCOM, and MARFORCYBER. Maj Hylant works at a leading software virtualization company building integration capabilities to enhance lethality in cyber.

Failed domestic policies and strategies have allowed the cyberspace warfighting domain to be increasingly, if not wholly, reliant on foreign supply chains—mainly from China. This article evaluates the President's National Cyber Strategy of 2018, conducts an analysis of the cyberspace supply chain's threats and dangers, and makes recommendations on securing the cyberspace domain.

Failed and Failing Strategy

The President's National Cyber Strategy of 2018 addresses many of the security concerns that the DOD and the United States face as a whole. Still, it only briefly identifies and, for the most part, glosses over the United States' most critical vulnerability: reliance on foreign hardware manufacturing from China. The strategy states explicitly that it will promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards.[1] However, it fails to identify and address U.S. reliance on foreign hardware acquisitions and procurements. Chinese hardware at the microelectronic component level through complete electronic systems comprises most of the cyberspace infrastructure. It represents 90 percent of the world's smartphones, computers, and other electronics.[2] Reliance on more than 90 percent of the supply from one country is not a sustainable supply chain approach. Ironically, China understands the need for self-reliance in cyberspace supply chains and is attempting to remove the United States as part of its microelectronic supply chain. Communist leaders see advanced technology as a path to prosperity and to restoring China's national greatness. Xi Jinping is quoted as, "Self-reliance is the base of the struggle for the Chinese nation to stand among the peoples of the world."[3] The Chinese know that their technology is behind the United States when it comes to technical advancement, and they will steal what they do not have. On multiple stages, Gen Alexander has described the Chinese theft of American intellectual property, which is the "greatest transfer of wealth in history," likely costing the United States upward of $400 billion per year.[4]

Threats and Dangers

Often overlooked and misunderstood is how aggressive China is in the cyberspace domain. China is using cyber espionage for military and economic advantages. In 2018, the Justice Department estimated that more than 90 percent of economic espionage cases involved China, and more than two-thirds of the cases involved the theft of trade secrets were connected to China; this is in spite of China's 2015 pledge not to use espionage for their economic benefit.[5] One primary attack vector that could be easily used by China is a supply chain attack where counterfeited electronic parts are intentionally introduced into the supply chain. The key to understanding a supply chain attack is understanding what constitutes a counterfeit part and how parts can be injected into the system. A counterfeit electronic component is defined as an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer or a source with the express written authority of the original manufacturer or current design activity—including an authorized aftermarket manufacturer.[6] As per the Federal Acquisition Regulations definition, China has, in fact, intentionally infected U.S. cyberspace interests with compromised hardware. During a top secret probe, which remained open more than three years, investigators determined that counterfeit chips allowed the attackers to create a stealth doorway into any network that included the altered machines. Multiple people familiar with the matter say investigators found that the chips had been inserted at factories run by manufacturing subcontractors in China.[7] Since most U.S. original equipment manufacturers manufacture in China, there is a much higher likelihood of inserting intentionally compromised equipment with backdoors into the U.S. supply chain at U.S.-operated facilities in China.

Broken Policy with Good Intentions

The United States needs a whole of government and industry approach to break the dependence of Chinese manufactured micro electrotonic parts. Small policy advancements such as the Trade Agreement Act (TAA) have proven incapable and inefficient when trying to break the reliance of foreign original equipment manufacturers and U.S. corporations that manufacture in China. One example of a failed TAA regulation is the policy stipulation: provide a certificate of origin or certification from the manufacturer verifying that all products represented as manufactured in the United States or a designated country are TAA-compliant.[8] Ultimately, this policy has done nothing to prevent Chinese manufacturing but instead introduced an additional step into the process: the assembly of Chinese components in the United States with a "Made in the USA" sticker on the device. The policy fails to address where sub-components are manufactured. Components of the size of a grain of rice, which can create vulnerabilities into a network, may now have "Made in the USA" on them. Ultimately, if the United States wants to remove China from the supply chain, U.S. corporations have to return manufacturing to the United States. At this time, the incentives to move micro-electrotonic manufacturing back to the United States do not exist. The United States will need a significant paradigm shift of the corporate tax code, laws, and incentives to protect our supply chains that, at this time, are too arduous to overcome.

Conclusion

The hyper reliance on Chinese hardware, coupled with inadequate U.S. policies and strategies, should be alarming to U.S. policymakers, legislators, senior government officials, and American citizens. Increasing U.S. reliance on China for microelectronics while China is strategically and systemically attempting to remove the United States from Chinese supply chains can be likened to the pre-positioning of a Pearl Harbor-like cyber event. U.S. national security is becoming ever more threatened by China as each day goes by. Outside of the attack vectors mentioned in this article, China has an even easier alternative. They could simply cut off all micro-electronics exports to the United States, which would hold the Nation hostage for years to come in the cyberspace domain. If the United States does not immediately address these strategic gaps in policy, China will surpass the Nation as a near-peer adversary in all warfighting domains.

Notes

1. Office of the Presidency, *National Cyber Strategy 2018,* (Washington, DC: 2018).

2. Joe McDonald, "China Push to End Reliance on U.S. Tech at Trade Fight's Core," *AP News,* (July 2018), available at https://apnews.com.

3. Ibid.

4. Megan Henney, "Chinese Theft of U.S. Intellectual Property 'Greatest Transfer of Wealth' in History," *Fox Business,* (July 2018), available at https://www.foxbusiness.com.

5. David Vergun, "DOD Works to Increase Cybersecurity for U.S., Allies," *DOD News*, (September 2020), available at https://www.defense.gov.

6. Staff, "Defense Acquisition Regulations System, DOD," (Arligton, VA: n.d.).

7. Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg,* (October 2018), available at https://www.bloomberg.com.

8. Hope Lane, "GSA Boosts Enforcement of Trade Agreements Act (TAA)," *Aronson,* (May 2016), available at https://aronsonllc.com.