Fortifying U.S. Information and Communications Technology (ICT) Supply Chains

This National Counterintelligence and Security Center (NCSC) Supply Chain Spotlight focuses on counterintelligence (CI) and security concerns highlighted in the stated risks to the U.S. Information and Communications Technology (ICT) supply chain from the joint Secretary of Commerce-Secretary of Homeland Security one-year ICT Supply Chain Report (Report). This report was developed in response to E.O. 14017, *America's Supply Chains*, which identified the ICT supply chain as critical to ensuring our economic prosperity and national security. Above all other supply chains, the ICT supply chain supports other critical supply chains, which is why it remains a high-value target for nation-state actors.

CI Threats:

Outsourcing ICT Hardware Production

Sending ICT hardware manufacturing offshore creates multiple security vulnerabilities to the ICT supply chain. The Report states that ICT hardware manufacturing is primarily outsourced to and concentrated in Asian countries, particularly China. This outsourcing creates an overreliance on China to manufacture the hardware required in ICT products, which creates major vulnerabilities to the ICT supply chain. Specifically, the hardware outsourcing creates a higher probability that foreign adversaries have the opportunity to insert untrusted and/or counterfeit components into the hardware during the production life cycle. U.S. agencies do not have oversight on this hardware manufacturing process. Untrusted or counterfeit hardware components create critical risks such as system reliability issues, data theft and manipulation, malware dissemination, and persistent unauthorized access within networks. Moreover, when an ICT supply chain is geographically concentrated in a specific country, like China, supply chain disruptions can occur from state-sponsored nefarious tampering.

Open Source Software

The Report highlighted how the ICT software "ecosystem" relies heavily on open-source software, with 75 percent of all audited codebases in 2020 containing at least one open-source component and open-source software comprising 70 percent of the overall code. Unlike proprietary or "closed" software, which restricts who can access, use, and change the source code, open-source software is source code that anyone can inspect, modify, and is obtained by accessing a software library. For example, the zero-day vulnerability involving the Log4j vulnerability was open-source software. The Log4j vulnerability allowed malicious attackers to execute code remotely on any targeted computer and easily steal data or take control over an infected system. The Cybersecurity and Infrastructure Security Agency (CISA) Director, Jen Easterly, stated that the Log4j vulnerability was the "most serious" she had seen in her career and could take years for security professionals to address the fallout from the Log4j Vulnerability.[1] This is just one example of how an open-source software compromise can cause major disruptions.

[1] Interview by Eamon Javers with CISA Director Jen Easterly, CISA director says the LOG4J security flaw is the "most serious" she's seen in her career, December 16, 2021, CNBC (CISA director says the LOG4J security flaw is the "most serious" she's seen in her career (cnbc.com).

Structural Vulnerabilities

Structural vulnerabilities across ICT supply chains present several CI risks, including the lack of a domestic ecosystem for many ICT production segments and an overreliance on single-source and single-region suppliers. First, the lack of a U.S. ICT production ecosystem enables countries in Asia, particularly China, to advance its own manufacturing capabilities and associated ICT infrastructure, causing numerous CI supply chain risks. For example, China has multiple broad and ambiguous laws that give Chinese officials sweeping authority to demand sensitive information from business operating in China. These laws compel foreign and domestic firms operating in China, or doing business with a company operating in China, to share certain data with Chinese authorities on request, giving the Chinese unfettered access to company records and files, business contracts, and intellectual property. The lack of a domestic ICT ecosystem provides the Chinese government an opportunity to use these ambiguous laws to gain an ICT technological edge. Finally, single-source providers and single-source regions create CI risks similar to outsourcing, described above. Single-source providers and single-source regions create points of failure, which in turn can cause the entire operation to cease performing.

External Risks to the ICT Industrial Base

Finally, there a multitude of external risks to the ICT supply chain. The Report states that the current ICT supply chain leaves the United States overexposed to a variety of externally-derived risks that must be monitored to prevent serious disruption to the ICT supply chain. Specifically, the report highlighted insider threats to the ICT supply chain, software supply chain compromises from cyber-attacks, overextended third-party suppliers with insufficient security mechanisms exposing sensitive data to malicious actors, and state-sponsored cyber intrusions from countries opposed to U.S. interests resulting in intellectual proprietary theft or supply chain disruptions. These are just a few external risks to the ICT supply chain outlined in the Report.

NOTE: This NCSC Supply Chain Spotlight summarizes relevant information from the subject report to highlight counterintelligence and security issues. Please review the report in full to understand all supply chain risks identified by the authoring department. Assessment of the Critical Supply Chains Supporting the U.S. ICT Industry | Homeland Security (dhs.gov)