Information and Communications Technology and the Supply Chain Risk

Developed nations rely on technology for all types of industries, from communications to entertainment, safety to medicine, transportation to national security. Technology is so commonplace that consumers do not question where or how the technology in computers, phones, televisions, or other devices is sourced. What many around the world do not realize is that numerous components, often from across the world, go into creating these devices. This paper analyzes Information and Communications Technology (ICT) supply chain vulnerabilities and suggests steps to mitigate and strengthen the ICT supply chain.

Information and Communication Technology Supply Chain and Associated Risks

The National Institute of Standards and Technology (NIST) defines "supply chain" as "a system of organizations, people, activities, information, and resources, possibly international in scope that provides products or services to consumers."[1] Supply chains are not a new concept; however, the technology boom in the last century introduced a new set of risks, specifically to the ICT supply chains and the technology companies within these supply chains. Most technology companies operate on a global scale, where development, manufacturing and

[1] Nat'l Institute of Standards and Tech., *Computer Security Resource Center,* Glossary. From supply chain - Glossary | CSRC (nist.gov).

production are not constrained by borders or regions. However, this global ICT supply chain footprint introduces new risks to the ICT supply chain, such as introducing malicious code into ICT software, manipulating ICT hardware and firmware, and conducting denial-of-service (DoS) attacks on an ICT network that, in turn, disables an entire ICT infrastructure.[2]

The ICT field is incredibly broad, so this paper will only discuss three main ICT elements: hardware; firmware, and; embedded systems. It will discuss the vulnerabilities to the design and production of these three ICT elements across the supply chain.

Hardware refers to the physical components of a computer. Generally, hardware entails the motherboard, the hard drive, and/or random-access memory ("RAM") within a device.[3] Hardware also includes "computer chips, which process and complete the work needed to perform a given task" within the computer.[4]

Next, firmware is "the essential, embedded software needed for basic hardware operation."[5] Firmware functions as a "software program or set of instructions programmed on a hardware device [providing] the necessary instructions for how the device communicates with the other computer hardware."[6]

Finally, embedded systems integrate both hardware and firmware components. Typically, an individual microprocessor board contains embedded systems, with the system's programs stored in read-only memory ("ROM").[7] Nearly all devices with a digital interface contain embedded systems, including cars, televisions, and "smart" watches.[8] Embedded systems are found in almost every device, making them susceptible to malicious sabotage. For example, Paul Kocher, a cybersecurity subject matter expert, stated "embedded systems often provide critical functions that could be sabotaged by malicious parties [by] send[ing] or receiv[ing] sensitive or critical information using public networks or communications channels accessible to potential attackers..."[9]

---

[2] *Id*.
[3] Merriam-Webster (n.d). Hardware. *Merriam-Webster.com dictionary*. (March 2022) https://www.merriam-webster.com/definition/hardware).
[4] David Inserra, and Steven Bucci, *Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace*, p.2. The Heritage Foundation Backgrounder. (March 6, 2014) (http://thf_media.s3.amazonaws.com/2014/pdf/BG2880.pdf).
[5] *Id*.
[6] P. Christensson, *supra*.
[7] V. Beal, Embed systems definition, Webopedia, (http://www.webopedia.com/TERM/E/embedded_system.html). *See also* Microprocessors control the logic of almost all digital devices. *Id*. ROM stands for read-only memory and once data has been written onto a ROM chip, it cannot be removed. *Id*
[8] *Id*.
[9] P. Kocher, et al., *Security as a New Dimension in Embedded System Design.* (June 7, 2004) (http://www.princeton.edu/~rblee/ELE572Papers/Fall04Readings/SecurityEmbeddedSystemsDAC.pdf).

Hardware, firmware, and embedded systems are all vulnerable and at risk within their respective supply chains. The Defense Federal Acquisition Regulation Supplement ("DFARS"), § 806 states that a "supply chain risk" is the

> …risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.[10]

Attempting to secure an ICT supply chain can be extremely difficult and tedious. Examining both a computer chip's supply chain and the difficulty in securing that supply chain provides an excellent supply chain risk case study since computer chips are in almost all technology devices. Computer chips enable functionality to small devices, like cell phones and personal computers, as well as manage large infrastructures like power grids, and typically, can only run properly if they are not infected with malicious software (malware).[11] Chip design is a global enterprise, with more than 1500 companies in the world dedicated to chip production and manufacturing.[12] The full "chip ecosystem," consisting of producers, engineers, individuals, and entities that purchase these products, all rely on the supposition that chips are reliable and secure.[13] Since the majority of chip hardware cannot be changed once the chip leaves the factory,[14] most malware "can only be inserted by someone who can access and alter the design before it is manufactured and placed in a product."[15]

Moreover, "the design process for a single chip can involve contributions from hundreds of people, many of whom may be employed by third-party companies that simply provide functional blocks and who have little or no stake or interest in the success of the chip."[16] Further, the number of people involved in the chip-making process is multiplied by global outsourcing. Outsourcing to third parties plays a key role in the chip design and production process and presents a more significant risk for malware insertion.[17] Though outsourcing is

---

[10] Def. Acquisition Regul. Sys., Department of Defense (DoD) (2012). Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk. (https://www.federalregister.gov/documents/2013/11/18/2013-27311/defense-federal-acquisition-regulation-supplement-requirements-relating-to-supply-chain-risk-dfars).

[11] John Villasenor, *Ensuring Hardware Cybersecurity.* Brookings Institute (May 2011). (http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity)

[12] *Id*.

[13] *Id*.

[14] A Field Programmable Gate Array (FPGA) is an example of a programmable integrated circuit that is designed to be configured by a customer or a designer after manufacturing.

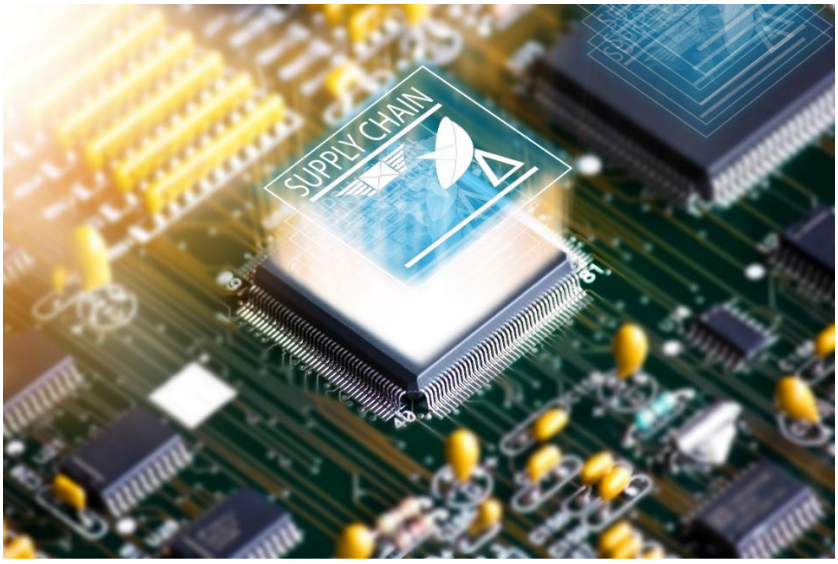
[15] *Id*.

[16] *Id*.

[17] *Id*.

more economical, "the combination of growth in both complexity and outsourcing means that the number of people with access to the design for a single chip during its development can easily number in the hundreds."[18]

Securing a chip against malware insertion is made even further difficult due to the chip's microscopic nature as it is difficult to quickly identify any alterations to the chip throughout the design and product process.[19] For example, the Federal Bureau of Investigation brought a 10-count indictment detailing how a Chinese telecommunications device manufacturer violated multiple confidentiality and non-disclosure agreements with its U.S. company partner by stealing trade secrets during the manufacturing process. Specifically, the Chinese manufacturer secretly took photos of proprietary property as well as took measurements of parts during the manufacturing process, and in one instance, stole pieces of the property so that Chinese engineers could try to replicate it.[20] Thus, as described above, it can be difficult to protect against vulnerabilities given the complexities of the ICT supply chain.



ICT Supply Chain Vulnerabilities

Due to the ICT supply chain's complex global nature, the threat of a potential "malicious attack" is constant, making it a crucial supply chain to safeguard. In 2012, the White House

[18] *Id*.
[19] *Id*.
[20] Department of Justice, Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice, (January 28, 2019) (Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice | OPA | Department of Justice).

commissioned the Government Accountability Office (GAO) to identify ICT supply chain risks within federal agencies and determine how national security related departments address them.[21] The GAO study concluded that global supply chain reliance led to many risks that could adversely affect government agencies' missions. The study identified four potential supply chain vulnerabilities that could result in hardware containing malicious code.[22] While initially commissioned for federal agencies, the GAO report applies to both the public and private sector and is still relevant today.

The four identified GAO vulnerabilities:

1. The lack of adequate testing for software updates and patches
2. Incomplete information on ICT suppliers,
3. The use of supply chain delivery and storage mechanisms that are not secure, and
4. The acquisition of information technology products or parts from independent distributors, brokers, and the gray market.[23]

The lack of adequate testing for software updates and patches

When system updates or patches go untested, the risk that an attacker could insert malware into the system increases.[24] An example would be an agency or contractor that "fails to validate the authenticity of patches with suppliers," leading to an attacker being able to write counterfeit patches that could allow unauthorized access to the system.[25] Lack of adequate testing for updates leaves devices vulnerable to the threat of the installation of hardware or software containing malware.

Incomplete information on ICT suppliers

Incomplete information on ICT suppliers occurs when ICT equipment is acquired without understanding the "supplier's past performance or corporate structure."[26] By not inquiring into the supplier's past performance, there are risks of deficient products or of an adversarial supplier attempting to access sensitive information. For example, without background knowledge as to who the supplier is, an agency acquiring ICT equipment would not know if the supplier or its employees "are subject to undue foreign ownership, control or influence."[27] Inadequate

---

[21] Gov't Accountability Off., *IT Supply Chain National Security-Related Agencies Need to Better Address Risks*. (March 2012) (https://www.gao.gov/assets/590/589568.pdf).
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *Id*.
[27] *Id*.

information regarding the ICT supplier leaves devices vulnerable to malware and counterfeit software or hardware; the acquisition entity is therefore vulnerable to reliance on a malicious or unqualified service provider.

The use of supply chain delivery and storage mechanisms that are not secure

The use of supply chain delivery and storage mechanisms that are not secure causes an increased risk that the ICT product could be threatened while in transit to the purchaser.[28] This vulnerability could allow "a[n] [attacker] to gain unauthorized access to the ICT product, thereby facilitating unauthorized modification, substitution, or diversion."[29] Ultimately, this could lead to the exposure of sensitive information without the knowledge of the purchaser. The use of unsecure delivery and storage mechanisms leaves devices vulnerable to the threat of the installation of hardware or software containing malware, and the installation of counterfeit hardware or software.[30]

The acquisition of information technology products or parts from independent distributors, brokers, and the gray market

Acquiring ICT products from independent distributors, brokers, and the gray market increases the risk of encountering substandard, subverted, and counterfeit products.[31] Independent distributors purchase products so they can redistribute them back into the market without any contractual agreement with the original manufacturer. Here, the gray market refers to the "trade of parts through distribution channels that, while legal, are unofficial, unauthorized, or unintended by the original component manufacturer."[32] Dealing with independent distributors and brokers leaves devices vulnerable to counterfeit products and malicious code.

Despite these GAO findings, the United States has failed to address these vulnerabilities and has continued to expose itself to significant threats to the IT supply chain. For example, in 2014 Lenovo, one of the world's largest personal computer retailers began pre-installing Superfish software[33] into its products. Superfish allowed consumers to "shop for deals" on the web.[34] However, it also allowed attackers access to a person's internet traffic and browser history by intentionally "poking a hole" into the browser security, allowing anyone on the Wi-Fi

---

[28] *Id*.
[29] *Id*.
[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] David Auerbach, *You Had One Job, Lenovo*. Slate (Feb. 20, 2015) (http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html).
[34] *Id*.

network to easily hijack the computer browser.[35] Robert Graham, a cybersecurity expert from Errata Security, tested the Superfish vulnerability, and found it incredibly easy to attack. He was able to intercept the encrypted Superfish communications all while "hanging out near them at a café Wi-Fi hotspot" without the victims aware the attack was taking place.[36] [37]

In February 2015, the Department of Homeland Security (DHS) urged Lenovo consumers to uninstall Superfish and the connected Superfish certificates because the computers were "vulnerable to serious cyberattacks, including interception of passwords and sensitive data being transmitted through browsers."[38] Superfish Chief Executive Adi Phinas stated that the "vulnerability was inadvertently introduced by Israel-based Komodia, which built the application described in the government notice."[39] This is just one example of malicious code being surreptitiously inserted while the product was still in production.

Outsourcing Risks

The risk to U.S. national security posture greatly increases when U.S. companies outsource manufacturing to foreign states, especially to China and Russia. 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 Beijing unfettered access to company records and files, business contracts, and intellectual property. Additionally, Russia's lawful intercept system, the System for Operational Investigative Measures (SORM), enables the Russian Federal Security Services (FSB) to monitor, retain, and analyze all data that traverses Russian communication networks, including internet browsing, email messages, telephone calls and fax transmissions. Specifically, if requested by the FSB, companies located in Russia are required to grant access to all data that moves across a Russian communication network for analysis.

---

[35] *Id*.
[36] *Id*.
[37] Seth Rosenblatt, *Lenovo's Superfish Security Snafu Blows Up in its Face*. (Feb. 2015). (https://www.cnet.com/news/superfish-torments-lenovo-owners-with-more-than-adware/).
[38] Jim Finkle, *U.S. urges removing Superfish program from Lenovo laptops.* (Feb. 20, 2015). (https://www.reuters.com/article/us-lenovo-cybersecurity-dhs/u-s-urges-removing-superfish-program-from-lenovo-laptops-idUSKBN0LO21U20150220).
[39] *Id*.

Supply Chain Laws

In December 2018, President Trump signed the SECURE Technology Act into law.[40] Among other features, the law incorporates the "Federal Acquisition Supply Chain Security Act of 2018,"[41] creating the Federal Acquisition Security Council.[42] The Council's functions include, among others: 1) making recommendations to NIST regarding Supply Chain Risk Management ("SCRM") development standards; 2) creating procedures for information sharing, and; 3) setting criteria and procedures that can be used to exclude certain supply sources.[43]

Additionally, the Council develops policies and processes for all federal agencies to use in ICT acquisitions and engages with the private sector and other non-governmental stakeholders.[44] The law requires federal agencies to assess security risks in their supply chains when purchasing ICT products and authorizes the government to mitigate such threats by using "exclusion and removal" orders, for which the Council is to establish criteria and procedures.[45]

---

[40] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act. H.R. 7327, 115th Congress (2018): (https://www.govtrack.us/congress/bills/115/hr7327).
[41] Fed. Acquisition Supply Chain Sec. Act of 2018, S-3085, 115 Congress (2018). (https://www.congress.gov/bill/115th-congress/senate-bill/3085).
[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Tech. Act, *supra.*

The bill authorizes the Council to identify exceptions to the criteria for "exclusion and removal," make risk assessments, and identify how a source may mitigate the identified risk to get an order rescinded.[46]

On January 12, 2022 the U.S. Senate passed bipartisan legislation cosponsored by Senator Maggie Hassan (D-NH), Chair of the Emerging Threats Subcommittee, to help protect the United States against cybersecurity threats and other technological supply chain security vulnerabilities that arise when the federal government purchases services, equipment, or products. The Supply Chain Security Training Act would create a standardized training program to help federal employees responsible for purchasing services and equipment identify whether those products could compromise the federal government's information security. Currently, the legislation remains pending in the U.S. House of Representatives.

Mitigation

Promoting a more secure and resilient ICT supply chain will require significant effort from the U.S. Government, including considering the recommendations listed below. However, the U.S. Government alone cannot wholly accomplish this goal. The private sector and other non-governmental partners also must do their collective part to secure the ICT supply chain. ICT is a global industry, and ICT supply chain vulnerabilities are not confined to the United States. Addressing these challenges successfully will require close coordination and collaboration with international allies and partners.

To address the vulnerabilities and risks identified in the assessment, and to strengthen supply chain resiliency, the Secretaries of Commerce and Homeland Security recommend implementing the following strategy:

1. Revitalize the U.S. ICT Manufacturing Base: Support domestic investment and production of key ICT products, potentially including printed circuit boards (PCB) and semiconductors, through appropriate federal procurement incentives and program funding.

2. Build Resilience through Secure and Transparent Supply Chains: Promote supply chain risk management practices through procurement and monitoring efforts such as implementing an Assured Supplier Program for PCBs for the federal government and establishing a Critical Supply Chain Resilience Program at the Department of Commerce.

3. Collaborate with International Partners to Improve Supply Chain Security and Resiliency: Improve international engagements through existing fora to advance shared interests in the ICT industry. These interests include bolstering supply chain security and diversity

[46] Fed. Acquisition Supply Chain Sec. Act of 2018, *supra.*

for critical products, strengthening trade enforcement, and enhancing participation in international standards development.

4. Invest in Future ICT Technologies: Sustain the research and development (R&D) ecosystem through federal programs and legislation by supporting and expanding programs aimed at bringing nascent technologies to market as well as advancing manufacturing technologies.

5. Strengthen the ICT Workforce Pipeline: Support and expand programs that attract, educate, and train the ICT workforce by enhancing computer science curricula and investing in multiple secondary and post-secondary pathways, including through registered apprenticeships, career and technical education programs, and community college programs.

6. Engage with Industry Stakeholders on Resiliency Efforts: Strengthen public-private engagements to promote awareness and the adoption of risk mitigation techniques and best practices for securing the ICT supply chain.

7. Continue to Study the ICT Industrial Base: Conduct further industrial base studies on critical ICT products to monitor industry developments and guide long-term policy planning.[47]

[47] U.S. Dep't of Com. and U.S. Dep't of Homeland Sec., *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry*, (February 23, 2022) (https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry)

Conclusion

Supply chain attacks are a major concern to the federal government, and that concern continues to grow. Government agencies are dependent on ICT and require an uncompromised ICT supply chain to protect data and carry on their missions. More than ever, IT supply chains are increasingly difficult to assess or control, leaving government agencies vulnerable.

Combatting ICT supply chain vulnerabilities is not a quick undertaking. Until the ICT supply chain receives adequate resources and prioritization, attacks will be a constant threat. Safeguarding the ICT supply chain will require a more proactive, collaborative approach between private industry and federal and local governments in prioritizing and protecting its ICT supply chain.