SECURE TOMORROW SERIES TOPIC PRIMER: ICT SUPPLY CHAIN RESILIENCE

WHAT IS THE ICT SUPPLY CHAIN?

The information and communications technology (ICT) supply chain comprises the hardware and software that make up the Internet and telecommunications technology. From a hardware perspective, this supply chain provides physical components used in the construction of devices (e.g., personal computers) and other infrastructure (e.g., wireless networks, datacenters). From a software perspective, the supply chain consists of third-party repositories that developers use as well as software updates and upgrades for applications and operating systems. In addition, international standards-setting bodies provide the standards that underpin ICT operations, such as Internet protocols that govern the format and ways data are sent from one computer to another over the Internet.

The ICT supply chain is rooted in mid-20th-century telecommunications technology. Initially, circuit-switched networks relied on a supply chain of phone lines, human operators, and analog devices. The advent of semiconductors in the 1960s enabled the invention of modern computing and networks that could communicate using data grouped in small packets, leading to the early Internet and digital computing devices. The early Internet relied on supply chains that included companies that developed semiconductors and academic institutions that developed Internet protocols. As semiconductors grew cheaper and more powerful, the modern Internet emerged and has become increasingly critical to both global commerce and critical operations (e.g., national defense). Meanwhile, the supply chains underpinning the Internet and other telecommunications technologies have grown more complex and international. As a result, managing the ICT supply chain to ensure security and operational continuity has become increasingly difficult.

WHY SHOULD PEOPLE CARE ABOUT ICT SUPPLY CHAIN RESILIENCE?

The pervasive ICT supply chain ensures accessible and reliable electronic communications to individuals, businesses, and governments. As untrusted systems and components proliferate within crucial information and communications technologies, the integrity of all National Critical Functions will be threatened due to the extreme interconnectedness and importance of these technologies in our daily lives. A variety of technological and governance solutions are necessary to ensure supply chain resilience and overcome challenges, such as insecure software development practices, difficulties in identifying counterfeit or compromised hardware, and vulnerabilities arising from potential market dominance by foreign ICT manufacturers.

WHAT IS DRIVING CHANGE IN ICT SUPPLY CHAINS THAT COULD LEAD TO EMERGING AND EVOLVING RISKS IN THIS DECADE?

Several issues and trends will affect the security and stability of the ICT supply chain in the next three to seven years, including the following:

- Malicious actors may use artificial intelligence to facilitate cyberattacks, such as using enhanced malware to avoid detection, increase its rate of proliferation, conceal how compromised devices are being controlled, and exfiltrate data efficiently.
- Foreign manufacturers may potentially achieve market dominance in 5G components.
- The lack of testing for third-party software and hardware components will remain a problem, as will the expansive black market for compromised physical components.
- Due to geopolitical pressures, global supply chains may shift to domestically controllable supply chains to enhance national security.

- The use of edge computing and software-defined networks will likely increase.
- The United States will likely compete for influence in international Internet standard-setting bodies.
- As device and computational demands grow, the United States will likely be challenged to provide reliable energy.