Risk Mitigation Consulting Inc.

Intelligence and Analysis Division

WHITE PAPER SERIES

Risks to DoD Supply Chain

June 2020

INTENT

This white paper is designed to provide analysis of relevant, publicly available information on threat and hazard events/trends and their potential impacts to the interests of the United States, both at home and abroad. This product is not intended to be an all-encompassing assessment of the subject.

Risks to DoD Supply Chain

Introduction

The majority of the Department of Defense's (DoD) supply chain management is overseen by the Defense Logistics Agency (DLA). Headquartered in Fort Belvoir, Virginia with six major subordinate commands, the DLA manages nine supply chains to fill orders and dispatch shipments to both deployed and non-deployed DoD forces and installations, along with FEMA, DHS, GSA, and select foreign military clients. The supply chains include everything from food to raw materials to complete weapon systems for multiple terrains. Risks to the DoD's supply chain are ever-present. The DoD has contracts with thousands of vendors and independent contractors of all sizes, from small businesses to established telecommunications and information technology companies. Not all of those businesses observe the same standards of security, cybersecurity, and supply chain management that the DoD recommends. Disruptions can occur as a result of unforeseen events, such as meteorological, geological, or biological emergencies, along with logistical mishaps. They can also be the work of threat actors. The Office of the Director of National Intelligence (ODNI) has also emphasized risk management with a comprehensive approach to the elements of the modern DoD supply chain.[1,2,3,4]

Definitions

Supply chain management for the DoD is not as simple as filling orders for assets and securing them with locks and guards. Prior to the advent of modern networking systems, protecting the supply chain was a matter of physical security and access. The process of identifying vulnerabilities and mitigating risks in the modern supply chain is far more complex than just preventing theft, unauthorized access, or accidents. The ODNI identifies the components of the DoD's supply chain as the people, processes, technologies, information, and resources that deliver a product or service. Most of those are now online, creating numerous vulnerabilities that would not have been present even 30 years ago. Protecting information, tools, methodologies, and technologies is just as important as securing a weapons system from espionage or theft. Threat actors that seek to exploit vulnerabilities can come from foreign nation states, foreign intelligence entities, terrorist groups, and criminal organizations. Disruptions can include traditional attacks on physical assets and security, but also logistical and economic moves such as sanctions, tariffs, and embargoes. Cyberattacks and other attempts to compromise cybersecurity also pose an omnipresent threat. For a foreign nation state, stealing a physical asset is not nearly as desirable as accessing plans and documentation in order to manufacture the asset for itself, or creating a backdoor to maintain continued access to communications and information. While the DoD does everything it can to mitigate risk and observe good "cyber-hygiene," creating an airtight system is impossible. Independent contractors may not meet the department's standards. Their subcontractors (and those company's subcontractors) may introduce unforeseen variables or create new opportunities for would be threat actors. [5,3,4]

Potential Threats to the DoD Supply Chain

In 2018, the Government Accountability Office (GAO) released a report that identified five threats that the Federal supply chain faces, particularly regarding information technology. The first is the installation of intentionally harmful hardware or software. The second is the installation of counterfeit hardware or software. The third is a failure or disruption in the production or distribution of critical products. The fourth is unknowing reliance on malicious or unqualified service providers for the performance of technical services. Finally, the fifth is the installation of hardware or software containing unintentional vulnerabilities, such as defective code. Many of these same principles also apply to non-IT items and services. However, they are all caused by either malicious actors and/or a failure of oversight. Overall DoD supply chain management has improved over the years, but smaller contractors and subcontractors continue to present challenges. The DoD issues the Defense Federal Acquisition Regulation Supplement, which outlines minimum security standards. However, enforcement of those standards among smaller vendors has been difficult.[6,4]

The installation of intentionally harmful hardware or software is, by definition, the work of a threat actor working on behalf of a foreign nation state, a foreign intelligence service, a criminal organization, or a terrorist group. While Amazon was considering acquiring Elemental Technologies, a DoD contractor, Amazon discovered a microchip on the company's servers which was designed to provide a backdoor for hackers. The chip was inserted at factories run by manufacturing subcontractors in China. Elemental's servers were already in use in numerous DoD and CIA assets.[7]

While federal law requires agencies to purchase a majority of items manufactured in the United States, this becomes more complicated when component parts may, themselves, have been manufactured elsewhere. While the example of Elemental is the most egregious, these unknown values within the supply chain also enable unscrupulous subcontractors or secondary vendors to use counterfeit or generic parts of dubious quality. A server might have been assembled in California, but its motherboard was purchased from China, where the manufacturer cut costs by using counterfeit microchips.[8,9]

The failure or disruption of the DoD supply chain can be caused by the same threat actors mentioned before. Supplier nations may also hinder or cease sales to the United States as part of a trade dispute. However, it can also be disrupted by meteorological, geological, and biological events. Recently, the COVID-19 pandemic caused factory closures in Mexico, India, Italy, and Spain. The DoD had contracts with vendors that relied on overseas suppliers for particular parts, with no contingency available. When factories closed because of local health codes or worker illness, parts became unavailable. China's export of rare earth minerals to the United States has also been disrupted by the pandemic and ongoing trade disputes. Rare earth minerals are necessary for the production of everything from telecommunications equipment to weapons systems. The DoD, along with Congress and other federal agencies, has prioritized domestic mining operations for the past three years. As of June 2020, the supply chain from China is still less reliable than it used to be.[10,11]

In the case of Chinese telecom provider Huawei, the Federal government banned companies from using its networking equipment in 2012, then added it to the Department of Commerce's Bureau of Industry and Security Entity List in May 2019. An executive order from President Donald Trump effectively banned Huawei from U.S. communications networks, which has been extended to 2021. The Federal government, including the DoD, and its contractors are forbidden from using Huawei components. These actions were born out of concern for the company's disputed relationship with the Chinese government. Thus, the DoD protected its supply chain by avoiding a potentially malicious service provider.[12,13,14,15]

In 2019, the Inspector General of the Department of Defense issued an audit of the DoD's management of cybersecurity risks. The report detailed "purchases of [commercial off-the-shelf, or COTS] information technology items for the Army and Air Force and determined that GPC holders purchased at least $32.8 million of COTS information technology items with known cybersecurity risks in FY 2018." These included a vulnerability in Lexmark printers which allowed for the execution of malicious code. Large purchases of COTS hardware and software may save the DoD an enormous amount of time and money, but it also multiplies vulnerabilities and increases the likelihood of widespread exploitation. Banning the purchase of COTS hardware and software would be impractical in the extreme. It falls to the DoD to research existing and potential vulnerabilities on an ongoing basis.[16]

Case Studies

The following case studies detail disruptions to the DoD supply chain, insofar as they affect its mission, assets, and personnel. The following cases do not constitute an all-inclusive list of disruptions, but rather they provide a baseline overview of threats to the DoD.

Elemental

In 2015, Amazon was considering the acquisition of a startup in Portland, Oregon called Elemental Technologies. Amazon wanted Elemental for its work with compressing streaming video, as its Prime streaming service was in development. Elemental already had government contracts, including providing servers used in DoD data centers, in the Navy's aircraft carriers, and in the CIA's unmanned aerial vehicles (UAVs, or drones). The servers were assembled by a subcontractor called Supermicro Computer, Inc., located in San Jose, California. Amazon commissioned a routine security check of the servers while it considered purchasing Elemental. An independent audit found a type of embedded microchip on the servers' motherboard that would allow hackers to access networks connected to the servers. The motherboards were manufactured in China.[7]

DoD officials anonymously confirmed to the media that the microchips were placed by an espionage unit of the People's Liberation Army. The motherboards were in use by not only the DoD, but 30 private companies, including Apple. Amazon acquired Elemental in September 2015 and later denied that it had uncovered the microchips. Apple and Supermicro also denied finding the chips, although the tech giant later severed its relationship with the vendor. DoD and other government officials strongly disputed the companies' denials. The microchip resulted in additional trade sanctions against China. Tech companies have been encouraged to seek other options in their supply chain.[7]

Huawei

The United States banned companies from using Huawei networking equipment in 2012 amid controversy over the company's relationship with the Chinese government. Huawei maintains that it is independently owned by its employees. Independent research published in April 2019 found that the company is owned 1.01% by founder and chief executive Ren Zhengfei and 98.99% by a "trade union committee." In China, these entities report to more senior national trade organization that are run by the government. Huawei claims this is a matter of compliance and that the trade union committee does not oversee company operations. Huawei was added to the US Department of Commerce's Bureau of Industry and Security Entity List in May 2019 via executive order, effectively banning the company from US communications networks. The order has been extended until 2021, but companies have been granted temporary licenses to work with Huawei on the development of the 5G standard.[17,15,12]

On 31 December 2019, the DoD issued an interim rule building on its own unique restrictions that prohibit it from doing business with Huawei or similar entities. Section 889 of the 2019 National Defense Authorization Act (NDAA) already prohibits the purchase or use of "covered telecommunications equipment or services," to include anything produced by Huawei or the ZTE Corporation. The expanded interim rule prohibits products from China and the Russian Federation, does not allow waivers, and imposes new stipulations for DoD Contractors.[18,19,20,21]

COVID-19

Even as the DoD tries to disentangle its supply chain from China, its vendors may rely on subcontractors selling components made there. Certain rare earth minerals and chemicals necessary for manufacturing are exported by China. Trade and travel restrictions meant to prevent the spread of COVID-19 have disrupted the DoD's supply chain, even from Canada and Mexico. The DoD is exempt from some restrictions and remains a strong customer for its vendors, especially as it requires large shipments of PPE for personnel. But many of contractors also serve the civilian market and have been required to comply with regulations. During the height of the pandemic, many companies and their suppliers were temporarily shuttered. By April, many had reopened but were hobbled by the weakened economy and reduced demand.[22,23]

To mitigate the damage of the economic downturn, the DoD increased progress payment rates to 90% for large businesses and 95% for small businesses. Lockheed Martin advanced over $50 million to small and medium sized businesses. However, the logistical issues created by the pandemic have remained. Employees are sick or have family members who are sick. Many companies are still allowing their staff to work from home. While progress payments and funds from the Paycheck Protection Act have assisted contractors during the pandemic, the supply chain has not returned to its former state.[24]

Outlook

It is incumbent upon the DoD and its contractors to rethink business continuity planning in the face of supply chain disruptions. Threats from malicious actors are ever-present, as are the risk of logistical mishaps and meteorological, geological, and biological events. COVID-19 is at the forefront of these concerns at the moment, but it is evident that the supply chain is being used by foreign nation states to spy on American networks, collecting data for analysis and even for intellectual property theft. All of the components of the DoD's supply chain have their own unique risks and vulnerabilities. Protecting the people, processes, technologies, information, and resources that make up the chain requires a different approach for each. The DoD, its assets, and personnel are at continued risk, as the challenges posed by the ascent of Huawei and COVID-19 are ongoing.

Sources

[1] Defense Logistics Agency. (2020, May). Defense Logistics Agency Fact Sheet. Retrieved on June 22, 2020, from https://www.dla.mil/Portals/104/Documents/Headquarters/DLA%20At%20A%20Glance/DLAFactSheetMay2020.pdf.

[2] Office of the Director of National Intelligence. (n.d.). Supply Chain Risk Management. Retrieved on June 22, 2020, from https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

[3] Office of the Director of National Intelligence. (2016, August 11). Know the Risk - Raise Your Shield: Supply Chain Risk Management. Retrieved on June 22, 2020, from https://www.youtube.com/watch?v=oj5iD0D7JsY&feature=youtu.be.

[4] Shacklett, M.E. (2019, April 29). DOD Steps Up Supply Chain Security Programs for Smaller Contractors. Retrieved June 22, 2020, from https://fedtechmagazine.com/article/2019/04/dod-steps-supply-chain-security-programs-smaller-contractors.

[5] Almloff, J. (2020, May 11). Government Helps its Supply Chain Build OT and IoT Cybersecurity. Retrieved June 22, 2020, from https://securityboulevard.com/2020/05/ government-helps-its-supply-chain-build-ot-and-iot-cybersecurity/.

[6] U.S. Government Accountability Office. (2018, July 12). Supply Chain Risks Affecting Federal Agencies. Retrieved June 22, 2020, from https://www.gao.gov/assets/700/693064.pdf.

[7] Robertson, J. & Riley, M. (2018, October 4). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Retrieved June 22, 2020, from https://www.bloomberg.com/news/features/ 2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[8] Ayres, T. (2020, May 22). The US Needs to Rethink its Overseas Supply Chain. Retrieved June 22, 2020 from https://www.defensenews.com/opinion/commentary/2020/05/22/the-us-needs-to-rethink-its-overseas-supply-chain/.

[9] U.S. Government Accountability Office. (1978, April 5). The Buy American Act. Retrieved June 22, 2020, from https://www.gao.gov/products/105519.

[10] Hudson, L. (2020, April 28). COVID-19 Alters DOD View of Supply Chain. Retrieved June 22, 2020, from https://aviationweek.com/defense-space/supply-chain/covid-19-alters-dod-view-supply-chain.

[11] Gramer, R. & Johnson, K. (2020, May 25). U.S. Falters in Bid to Replace Chinese Rare Earths. Retrieved June 25, 2020, from https://foreignpolicy.com/2020/05/25/china-trump-trade-supply-chain-rare-earth-minerals-mining-pandemic-tensions/.

[12] Keane, S. (2020, June 17). Huawei Ban Timeline: US Companies Allowed to Work with Huawei on 5G Standards. Retrieved June 22, 2020, from https://www.cnet.com/news/huawei-ban-full-timeline-us-restrictions-china-trump-executive-order-security-threat-5g-commerce/.

[13] Kastrenakes, J. (2018, August 13). Trump Signs Bill Banning Government Use of Huawei and ZTE Tech. Retrieved June 22, 2020, from https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

[14] Gartenberg, C. (2020, May 13). Donald Trump Extends Huawei Ban Through May 2021. Retrieved June 22, 2020, from https://www.theverge.com/2020/5/13/21257675/trump-extends-huawei-ban-may-2021-china-us-android-google-telecom.

[15] Tao, L. (2019, April 26). Who Controls Huawei? Chinese Telecoms Leader's Ownership Structure Explained in More Detail. Retrieved June 22, 2020, from https://www.scmp.com/tech/tech-leaders-and-founders/article/3007863/who-controls-huawei-chinese-telecom-leaders.

[16] Inspector General, U.S. Department of Defense. Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items. Retrieved June 22, 2020, from https://media.defense.gov/2019/Jul/30/2002164272/-1/-1/1/DODIG-2019-106.PDF.

[17] Team A.A. (2020, March 2). The Huawei and US Debacle: The Story so Far (Updated March 2). Retrieved June 22, 2020, from https://www.androidauthority.com/huawei-google-android-ban-988382/.

[18] Burrows, R.N. & Chiarodo, J.A. (2020, January 6). United States: A DoD New Year's Resolution: No More Covered Chinese (And Possibly Russian). Retrieved June 22, 2020, from https://www.mondaq.com/ unitedstates/telecoms-mobile-cable-communications/880358/a-dod-new-year39s-resolution-no-more-covered-chinese-and-possibly-russian.

[19] Blank Rome, LLP. (2019, October 7). 5 Tips for Complying with New Section 889 Supply Chain Regulations. Retrieved June 22, 2020, from https://www.blankrome.com/publications/5-tips-complying-new-section-889-supply-chain-regulations.

[20] Federal Register. (2019, December 31). Defense Federal Acquisition Regulation Supplement: Covered Defense Telecommunications Equipment or Services (DFARS Case 2018-D022). Retrieved June 22, 2020, from https://www.federalregister.gov/documents/2019/12/31/2019-27824/defense-federal-acquisition-regulation-supplement-covered-defense-telecommunications-equipment-or.

[21] U.S. Congress. (2018, August 13). John S. McCain National Defense Authorization Act for Fiscal Year 2019. Retrieved June 22, 2020, from https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

[22] Ayres, T. (2020, May 22). The US Needs to Rethink its Overseas Supply Chain. Retrieved June 22, 2020, from https://www.defensenews.com/opinion/commentary/2020/05/22/the-us-needs-to-rethink-its-overseas-supply-chain/.

[23] Vergun, D. (2020, April 20). COVID-19 Plant Closures Affect DOD's Industrial Base. Retrieved June 22, 2020, from https://www.defense.gov/Explore/News/Article/Article/2156378/covid-19-plant-closures-affect-dods-industrial-base/.

[24] Shacklett, M.E. (2020, June 16). Lessons Learned: Covid-19 Impact on the DoD Supply Chain. Retrieved June 22, 2020, from https://www.eetimes.com/lessons-learned-covid-19-impact-on-the-dod-supply-chain/#.