SUPPLY CHAIN SECURITY – IT'S EVERYONE'S BUSINESS

by Ron Hodge, Robert A. Martin, and Michael Aisenberg

For more than half a century, or for as long as the United States has had what has been described as a Military Industrial Complex, the U.S. Defense Industrial Base (DIB) has identified challenges, dedicated resources toward solving them, and attempted to learn from past mistakes.

But when it comes to supply chain security, the United States continues to relearn painful lessons from the past without taking the necessary steps to prevent or mitigate these mistakes before they occur again. This is true even while the nature of many goods has evolved to a point where much of their functionality includes a software element. The DIB can no longer afford to continue making the same mistakes, repeatedly, with regard to safeguarding the nation's critical supply chains. Rather, the United States must create a comprehensively scoped approach to supply chain security tailored to the mission and technologies of concern that mitigates the potential impacts of a successful attack on a supply chain. Additionally, the defense industry must address the compromises in its supply chains regardless of whether they come from purposeful, accidental, or negligent conduct or sources. This requires the DIB and the national security community to determine what negative operational impacts stakeholders should try to avoid and use that to drive supply chain focus. And for the industrial base specifically, it must be made clear that failures to effectively address the various aspects of supply chain security will affect not only our national security posture but industry's own ability to conduct business with the United States government.

Supply chain security is at the center of many of today's national security challenges.[1] Few things illustrate this reality as well as the recent SolarWinds software supply chain hack where it was discovered that the U.S. has been the target of a massive Russian espionage campaign,[2] exploiting trust in information and communications technology (ICT) supply chains. In spring 2020, the SolarWinds company networks were penetrated by a state-sponsored attack. While on the SolarWinds systems and networks, the adversary learned how SolarWinds crafted, and created its software. With this understanding, the adversary developed a piece of malware that it implanted into the SolarWinds software build system, which, during the building of SolarWinds' Orion Network Management

Products, inserted malicious code (a trojan) that mirrored the SolarWinds coding style. The "trojaned" versions of the Orion products were downloaded as legitimate updates and new versions by as many as 18,000 domestic and international customers, including several U.S. government agencies and companies across several sectors that used SolarWinds products to help manage their systems and networks. The adversary waited for these infected copies to be installed and run, with the trojaned malicious code calling home to the adversary's server, announcing a possible target to explore. The adversary did not follow up on all trojaned Orion products but selected only some for further penetration and exploitation.

The nature of this sophisticated attack relied on the users' networks providing trust and privileges onto those systems, which allowed for the maligned program to be placed through the exploit of the compromised system's supply chain. Much like how the manner and details of how the metal for a high-speed, high-performance aircraft can be critical to the safe, secure, and reliable execution of the warfighting function, the secure and resilient development environment for commercial software is needed to keep it from being an exploit vector that undermines the operational integrity of U.S. organizations.

But the challenges for securing the DIB supply chain go beyond the digital frontier. For example, the early days of the COVID-19 pandemic shockingly left healthcare providers unable to secure N95 masks and basic supplies of personal protective equipment, while the nation experienced shortages of meat, toilet paper, and other staple goods. Long-standing systemic issues have been addressed only too late for the many Americans directly and indirectly affected by the pandemic. When looking at the supply needs for defense-related tasks, be they for humanitarian assistance, biomedical research, or major combat operations, these domestic supply chain vulnerabilities have illustrated the fragility of these complex and interconnected components, which threatens to impact Department of Defense (DoD) missions.

What the national security community seeks to address more comprehensively and consistently is the "appropriate due diligence" of the stakeholders in our complex supply chains.[3] As devastating as these ICT and physical supply chain threats are, they are merely examples of the increasing supply chain challenges we face in the global marketplace. Understanding how the U.S. defense base got to this point will help inform the challenges it currently faces in light of growing competition with near-peer nations like China. With that understanding, policy makers can begin to shape how supply chain security might evolve to maximize agility in resourcing while remaining resilient against disruption. Ultimately this should lead to the development and usage of comprehensive frameworks for analyzing and addressing the wider set of supply chain vulnerabilities.

From Full-Cycle Protection to Just-in-Time Supply

World War I was a global conflict that, among many other sobering lessons, showed the importance of managing and securing complex, interconnected supply chains. Compromise in munitions and combat material became a key concern as governments devised new strategies to contend with counterfeits and reduce opportunities for sabotage. The Anti-Tamper (AT) practice arose from this need to protect critical goods and services and is now considered one of many key components of the aggregate supply chain security practice. Today, AT is widely used for dealing with physical product security

WHILE TODAY'S SUPPLY CHAINS ARE OFTEN BUILT TO MAXIMIZE EFFICIENCY AND REDUCE COSTS, THEY GENERALLY SUFFER FROM REDUCED RESILIENCY TO UNEXPECTED EVENTS AND DISRUPTIONS.

and has evolved to include sophisticated techniques for tamper-proofing software and digital products.

With the introduction of nuclear, radar and sonar technologies, munitions, and other defense industries in World War II, it became existentially more important for the U.S. to secure the full lifecycle of critical infrastructure products and services. The tradeoff between the relatively high costs of securing these supply chains versus the criticality of impacts from a compromised product or service meant that the U.S. had to develop new capabilities for eliminating or managing these risks. These new methods and understandings, developed by the DIB during this period and into the Cold War era, offer us opportunities to apply some of those relevant techniques to today's supply chain challenges.

While today's supply chains are often built to maximize efficiency and reduce costs, they generally suffer from reduced resiliency to unexpected events and disruptions. Much of this fragility in the supply chain stems from just-in-time (JIT) manufacturing models that came to favor in the 1980s, and is exasperated now with globalization and the explosion of foreign-made and remotely created components into increasingly complex and brittle commercial global supply chains.

An example of this fragility is seen in the cascading effects that can be traced back to the blockage of the Suez Canal by the container ship Ever Given. For six days in March 2021, the waterway was completely blocked off because of a grounded ship, leaving this vital trade route unavailable to waiting vessels. Aside from the direct impacts to trade, secondary effects of the blocked canal included ports jammed with waiting ships and other vessels being in the wrong place for the next leg in their scheduled routes, resulting in downstream delays in accessibility of finished goods and materials. It also further contributed to the problem of shortages in packaging and containers resulting from the COVID-19 buying boom.

The DoD and the DIB have, in the past, responsively developed tools and processes to address supply chain security issues that have emerged in a changing technological, global economic, and threat environment. Each offers components that can be leveraged in today's cyber-enabled ecosystem and enhanced to address new challenges stemming from JIT and global supply chains. New challenges, new threats, and new environments demand a fresh look to enable a more comprehensive approach to securing modern global supply chains.

Competitor-as-Supplier

The 21st century has seen the maturing of the information economy, which itself is critically dependent on commercial information and communications technology that is predominantly manufactured in the factories of one country, China. Additionally, modern defense systems include commodity components that are produced in these same factories and that were never designed or managed to be part of a larger national security infrastructure. Therefore, the development and manufacture of microelectronics (semiconductors) became a focus for dealing with supply chain compromise.

Part of the answer for the DoD was to establish vetted and trusted partner organizations. These

trusted relationships would be formed across the supply chain, from initial research and design to production with trusted foundries and commercial suppliers, to supply stocks and storage, and finally for policy and groups involved in deployment and installation. This approach offers significant costs and availability challenges and leaves much of the remaining ICT attack surface vulnerable to supply chain risks.

U.S. adversaries understand these vulnerabilities all too well and, operating within the expanding information economy, have greater means of injecting themselves into every conceivable stage of technology development, furthering both their disruptive and intelligence objectives. While attempts at accessing sensitive information from competitors are nothing new, novel information pathways have offered an exponentially greater attack surface, lowered barriers to access, and reduced risk.

China specifically has committed to a sustained campaign to threaten U.S. national security through intellectual theft, intelligence operations, and compromising product integrity. As stated by FBI Director Christopher Wray at a Hudson Institute event in 2020, "The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security." As the great power competition heats up between our two nations, the modern threat is growing.

With the increased threat from competitor nations, and the vectors of vulnerability increasing, the obligation of responding to sophisticated supply chain risks is of paramount concern, whether those risks are from external threat or from lapses in production integrity.

Recommendations for (Re)Securing the Supply Chain

- **The DoD and components should adopt policies that require the usage of techniques and tools, like bills of materials, in contracts and agreements to support origin analysis and other supply chain analysis and risk-reduction activities.**
- **The DoD and components should establish policy for adopting a standardized framework of supply chain security risks that they and their suppliers use in scoping contracts and agreements.**

The Importance of Managing Risk

A modern supply chain discipline demands that stakeholders go beyond the technical understanding of the risks and practical implementations of profound marketplace changes. As recent examples have shown, each supply chain threat is an independently critical element, the aggregate of which can be used to scope and define the new level of due diligence required for the modern practice. It therefore becomes important to transition from a position of treating these cases as exceptions, to instead engaging in practices that include addressing them as a matter of standard practice performed across the more comprehensive, but transaction-appropriate, risk space.

The DoD has an ever-heavier reliance on, and leveraging of, the adaptability and flexibility that software brings to our weapon systems, management and operations capabilities, and sensor abilities for attack, defense, and operations management. With increased dependency comes increased need for more thorough and disciplined attention to software's constitution, sourcing, and manufacturing details. Just as a dirty rifle, non-conforming ordnance, and poor training can negatively impact the effectiveness of a warfighting

unit, so too can software supply chain mistakes. Being blind to the origination of our software components, the rigor and hardening that may have been performed, or the thoroughness of the adversarial/hazard analysis that may have been applied during creation of our software, can reduce effectiveness as well as introduce vulnerabilities to our own systems at a time and place of the adversary's choosing.

There are many promising approaches to address these risks, including the introduction of software and hardware bills of materials[4] (BOMs), which are extremely useful for gathering of provenance and pedigree data to show the origins, chain of custody, and details of creation of the software components in our systems. BOMs and Software Bills of Materials (SBOMs) provide a machine-readable path, operating at machine speed, to verify and validate that the software meets the operational needs for security, integrity, and resilience—both in initial deployment and for subsequent updates. An SBOM can provide the specifics of the origins of the software components themselves, which can be used for more in-depth analysis of the threats those creators may pose to a specific operational capability, allowing for risk mitigations and alternatives to be considered.

Drafting the use of these and other techniques into existing and new contracts will require changes, but the efficiencies these new approaches can bring will significantly offset the costs of change that their adoption will incur. Organizations that employed SBOMs for their operational enterprise were able to identify and isolate their usage of the tainted SolarWinds Orion software within hours of being alerted and took immediate steps toward remediation, whereas those that did not employ these techniques spent months exploring the impact while remaining vulnerable.

At its core, modern supply chain security is intended to ensure that a "meeting of the minds," as legal agreements are constructed to establish, is reached despite dependence on other parties. This is true even when applied to the most sensitive national security–related exchanges. Increasingly, the sensitivity of sophisticated national security software, and other ICT, exposes these transactions to the sort of intentional misbehavior identified in the SolarWinds compromise and subsequent exploits. The supply chain security discipline highlights a continuing obligation to maintain a very high standard to ensure the security, safety, and integrity of these products even when a malicious foreign adversary may not be apparent at the time.

The heightened degree of software and microelectronics updates and maintenance involved in modern weapon, platform, building, and transportation systems and the need for appropriate supply chain security practices to address these "post-purchase" activities require a level of due diligence yet unfamiliar to many in the acquisition and sustainment communities. Going forward, it must become standard practice to ensure the integrity of supply chain security artifacts as they become part of the national security infrastructure, with these obligations extending across the entirety of the supply chain throughout the system's

lifecycle. As the world's largest investor in defense technology, the DoD still has great leverage to include these risk-reduction requirements from its suppliers and partners.

Approaches like those of hardware and software bills of material, as well as other techniques, have proven effective in increasing the overall security of organizations that employ them. While including these supply chain security solutions into requirements may impose initial burdens on the enterprise, they provide longer-term offsets that reduce net costs and drive investment.

The Need for Tailored Risk Assessment

Different technologies, including microelectronics, software, aircraft wings, food, pharmaceuticals, or even handbags, have specific attributes that matter within the context they are intended to be used or operated. This is true whether these technologies experience functional compromise from sub-standard quality issues, from counterfeit and operational and support implications, or from maliciously tainted items resulting in negative impacts that compromise their utility, operational use, or secondary consequences derived from it. Identification and measurement of the risk that something might be tainted, counterfeit, or not constructed following good hygiene practices on quality production of the goods in question is going to be calculated differently for different domains of industry and their differing types of products. The technical specifics of the item being assessed, along with the consequence of the risks associated with its usage, will be driven by the item's intended operational employment.

Organizations that have taken steps to conduct supply chain security assessments, which include determining what elements of risk the organization has established as most relevant to its domains, must determine the appropriate processes and remedies to bring their perceived risks to operations in line through appropriate supply chain security practices. End users understand best how products will operate in the real world and can raise red flags to identify consequences that can occur when non-conformance manifests itself.

Dealing with this aggregate set of challenges consistently and appropriately across the vast possible supply chain security risk space requires a common framework that is both comprehensive and tailorable. This framework, like that of MITRE's System of Trust™,[5] must appropriately address the technology or service of concern and include assessments into each company that would be providing products or services that have operationally significant impacts in the anticipated operating environments. Importantly, operational impacts will differ based on differences in context, in mission, and in the usage of the technology, product, or service, or in the level of dependence on the suppliers.

Conclusion

Learning from both past and emerging examples, the U.S. must more quickly adapt to the changing supply chain security landscape. This requires more holistic information sharing of how and where contested supply chain threats exist in order to determine how the community can take action with responsively developed tools and processes. Now more than ever, the impetus is there for government and industry players to address more comprehensively and consistently the appropriate "due diligence" of stakeholders in their supply chains. Dealing with the complex set of supply chain security challenges outlined above requires an approach that allows organizations to have a comprehensive, consistent, and repeatable methodology for evaluating supply chain-specific concerns and risks.

It must become standard practice to ensure the integrity of supply chain security artifacts as they become part of the national security infrastructure, with these obligations extending across the entirety of the supply chain throughout the system's lifecycle. Organizations must determine the appropriate processes and remedies to bring their perceived risks to operations in line through appropriate supply chain security practices. To meet this challenge, MITRE, working in the public interest, designed a framework as an overarching structure to organize the risk topics addressed by an organization's supply chain security efforts and assessments with a structuring of 14 top-level supply chain security risk areas[6] to provide a path toward consistency and sharing of timely insights and recommendations.

Historically, these supply chain considerations are considered a part of acquisitions and procurement processes. But modern supply chain security demands a broader approach in which early tradeoffs are understood and mitigated to fit within tailored risk profiles across the entire system lifecycle. This in turn leads to greater accountability through the acquisition and sustainment processes. Therefore, it is necessary for the acquisition and sustainment communities, as well as the greater community of stakeholders, to work toward greater understanding on how to connect and address those more comprehensive supply chain security requirements. In this new environment, supply chain security is everyone's business.

About the Authors

Ron Hodge, as a national security strategy and emerging technology lead at MITRE, provides strategic and technical leadership across multiple disciplines. He focuses on early identification of disruptive technologies and acts on opportunities to conceptualize and deploy new ideas to address the hardest challenges facing our nation.

Robert Martin leads supply chain security efforts within MITRE and with industry and is the elected chair of the Industrial Internet Consortium Steering Committee. Mr. Martin created the community standard for software security weaknesses used globally as well as over 40 global standards addressing the interplay of enterprise risk management, cybersecurity, and critical infrastructure protection.

Michael Aisenberg is former cyber policy counsel in MITRE's National Security practice, supporting DoD and U.S. Intelligence Community agencies as an expert on privacy and other constitutional issues in ICT practice. He is the chair of the American Bar Association's Information Security Committee and has been appointed to the National Conference of Lawyers and Scientists. He previously headed the Washington offices of Digital Equipment and VeriSign and today is a member of the D.C. Bar and admitted to practice before the U.S. Supreme Court

Special thanks to **Michael Ripley** and **Mark Seip** for their substantive review and thoughtful recommendations.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org.

References

[1] White House Executive Orders 14017 (America's Supply Chains), 14028 (Improving the Nation's Cybersecurity), and 14034 (Protecting Americans' Sensitive Data From Foreign Adversaries) collectively address critical supply chain security for key sectors and address physical good supply chains as well as software supply chains.

[2] U.S. Department of Homeland Security (DHS), Cyber Security and Infrastructure Security Agency (CISA), Alert (AA20-352A) "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," December 17, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-352a

[3] Due diligence, in the legal sense, includes the behaviors engaged in by parties to transactions informed by legal obligations to ensure that the product or service being acquired is one intended to be sold by the seller, intended to be received by the purchaser or acquirer, and fit for the purpose that both intend.

[4] Discovery for Software Bill of Material (SBOM) - Blog JDisc - The concept of a bill of materials comes originally from manufacturing where you have a plan of the piece of hardware on which you list all parts needed to construct and build the asset. A software bill of materials (SBOM) is the same, just for software—a list of all components that make up a piece of software. This includes open-source and commercial components, and libraries, but also the infrastructure and application services that a system is composed of.

[5] An example approach for systems-based risk assessment is MITRE's System of Trust™. This method defines, aligns, and organizes overarching concerns and risks that stand in the way of organizations' trusting suppliers, supplies, and service providers. It offers a starting point for comprehensive, consistent, and repeatable methodology and is based on decades of supply chain security experience, deep insights into the complex challenges facing U.S. procurement and operational communities, and broad knowledge of relevant industry and government supply chain security efforts.

[6] MITRE's contribution to addressing this issue is the System of Trust, which includes 14 identified risk areas for supply chain security spread across Supplies/Components, Suppliers, and Services. These risk areas include: Hygiene; Counterfeit; Malicious Taint; External Influences; Organizational Stature; Financial Stability; Maliciousness; Organizational Security; Quality Culture; Susceptibility; and Security Quality, Integrity, and Reliability of a Service.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®