4-2021

Cyber Supply Chain Risk Management: Implications for the SOF Future Operating Environment

J. Philip Craiger
Embry-Riddle Aeronautical University, philip.craiger@erau.edu

Laurie Lindamood-Craiger
Cubic Defense Applications, Inc

Diane M. Zorri
Embry Riddle Aeronautical University, mayed@erau.edu

Alan Estevez, Principal Deputy Undersecretary of Defense for Acquisition, Technology and Logistics, addresses U.S. Special Operations Command acquisition employees on current issues within the Department of Defense acquisition community during the Special Operations Forces Acquisition Summit held at U.S. Special Operations Command, MacDill AFB, FL, 30 October 2014. Photo by U.S. Air Force Staff Sergeant Angelita Lawrence.

The emerging Cyber Supply Chain Risk Management (C-SCRM) concept assists at all levels of the supply chain in managing and mitigating risks, and the authors define C-SCRM as the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information and operational technology products and service supply chains.

As Special Operations Forces increasingly rely on sophisticated hardware and software products, this quick, well-researched monograph provides a detailed accounting of C-SCRM associated laws, regulations, instructions, tools, and strategies meant to mitigate vulnerabilities and risks—and how we might best manage the evolving and ever-changing array of those vulnerabilities and risks.

Joint Special Operations University
7701 Tampa Point Boulevard
MacDill AFB, FL 33621

https://jsou.libguides.com/jsoupublications

JOINT SPECIAL OPERATIONS JSOU UNIVERSITY PRESS

ISBN 978-1-941715-51-2

JSOU Report 21-3 Cyber Supply Chain Risk Management Craiger/Craiger/Zorri JSOU

JOINT SPECIAL OPERATIONS UNIVERSITY

Cyber Supply Chain Risk Management: Implications for the SOF Future Operating Environment

J. Philip Craiger, Laurie Lindamood-Craiger, and Diane M. Zorri

JSOU Report 21-3

Joint Special Operations University and the Institute for SOF Strategic Studies (IS3)

The Joint Special Operations University (JSOU) generates, incubates, and propagates (delivers and communicates) ideas, education, and training for expanding and advancing the body of knowledge on joint and combined special operations. JSOU is a 'hybrid organization' that performs a hybrid mission—we are a 'corporate university:' an academic institution serving a professional service enterprise, 'by, with, and through,' the United States Special Operations Command (USSOCOM). As such, we are both a direct reporting unit to the Commander, USSOCOM, on all Combined Joint Special Operations Forces (CJSOF) education and leader development matters, as well as the educational and leader development component of the Command.

The JSOU Mission is that JSOU prepares Special Operations Forces professionals to address strategic and operational challenges, arming them with the ability to think through problems with knowledge and insight. **Our Vision** is to constantly strive to be(come) USSOCOM's "think-do tank," world-class leader in "All Things" CJSOF strategic and operational education, training, and leader development, and the advancement of knowledge on the utility of CJSOF, for the Nation. We pursue this mission and vision through our best-practice teaching & learning, research & analysis (R&A), and engagement & service-outreach operations, activities, and initiatives. We achieve these outcomes-based goals by providing specialized joint professional military education, developing SOF-specific and unique undergraduate, graduate, and post-graduate-level equivalent curriculum, and by fostering special operations-focused R&A and outreach, in support of USSOCOM objectives and United States national and global strategic goals.

JSOU carries forward its R&A roles and responsibilities led by, and through its IS3, where our efforts are guided and informed by the most current U.S. National Security, Defense, and Military Strategies, and the **USSOCOM Mission:** *USSOCOM develops and employs fully capable Special Operations Forces to conduct global special operations and activities as part of the Joint Force to support persistent, networked, and distributed global Combatant Commands operations and campaigns against state and non-state actors, to protect and advance U.S. policies and objectives.*

Joint Special Operations University

JSOU Press publications are available for download at https://jsoulibguides.com/jsoupublications.

Print copies available upon request by writing jsou_research@socom.mil.

Sharpening the Edge of SOF's Advantage: The All-Domain SOF Leader-Professional

Cyber Supply Chain Risk Management: Implications for the SOF Future Operating Environment

J. Philip Craiger, Laurie Lindamood-Craiger, and Diane M. Zorri

JSOU Report 21-3
The JSOU Press
MacDill Air Force Base, Florida
2021

Recent Publications of the JSOU Press

Mazar-e Sharif: The First Victory of the 21st Century Against Terrorism, JSOU Report 21-2, William Knarr, Mark Nutsch, and Robert Pennington

The Blurred Battlefield: The Perplexing Conflation of Humanitarian and Criminal Law in Contemporary Conflicts, JSOU Report 21-1, Patrick Paterson

Iranian Proxy Groups in Iraq, Syria, and Yemen: A Principal-Agent Comparative Analysis, JSOU Report 20-5, Diane Zorri, Houman Sadri, and David Ellis

Special Operations Forces Civil Affairs in Great Power Competition, JSOU Report 20-4, Travis Clemens

Informal Governance as a Force Multiplier in Counterterrorism: Evidence for Burkina Faso, JSOU Report 20-3, Margaret Ariotti and Kevin Fridy

Village Stability Operations and the Evolution of SOF Command and Control in Afghanistan: Implications for the Future of Irregular Warfare, JSOU Report 20-2, William Knarr and Mark Nutsch

On the cover. U.S. Marine Corps Corporal Railee Reed, a satellite controller with 9th Communication Battalion, I Marine Expeditionary Force Information Group, operates a very small aperture terminal-large at Marine Corps Base Camp in Pendleton, California, on 25 February 2020. Photo by U.S. Marine Corps Lance Corporal Isaac Velasco.

Back cover. Alan Estevez, Principal Deputy Undersecretary of Defense for Acquisition, Technology and Logistics, addresses U.S. Special Operations Command acquisition employees on current issues within the Department of Defense acquisition community during the Special Operations Forces Acquisition Summit held at U.S. Special Operations Command, MacDill AFB, FL, 30 October 2014. Photo by U.S. Air Force Staff Sergeant Angelita Lawrence.

April 2021.

ISBN 978-1-941715-51-2

Comments about this publication are invited and should be forwarded to the Director, Institute for SOF Strategic Studies, Joint Special Operations University, 7701 Tampa Point Blvd., MacDill AFB, FL 33621.

****

The JSOU Institute for SOF Strategic Studies is currently accepting written works relevant to special operations for potential publication. For more information, please contact the Director, Institute for SOF Strategic Studies at jsou_research@socom.mil. Thank you for your interest in the JSOU Press.

****

Contents

Foreword vii

About the Authors xi

Introduction 1

Chapter 1. Modern Warfighting Technologies and the Supply Chain Problem 7

Chapter 2. Supply Chains, Threats, and Mitigation Strategies 13

Chapter 3. The SOF Supply Chain Problem 23

Chapter 4. Government Regulations for C-SCRM 37

Chapter 5. The Hyper-Enabled Operator (HEO) and the Supply Chain 45

Chapter 6. SOF Acquisition 63

Conclusions and the Future of SOF Acquisition 69

Acronyms 73

Endnotes 77

Foreword

Advancements in information collection, communications, weapons, and their associated technologies have often propelled their wielding armies to extraordinary successes. These product advances and their supply chains have always required protections against exploitation, sabotage, and attack. In this monograph, the authors comprehensively describe this maxim as a requirement in today's increasingly compounded environment, and nowhere is this more evident than in the Department of Defense (DOD) cyberspace supply chain.

The authors have composed a well-researched monograph for laypersons, decision-makers, and leaders without technical government acquisition and procurement backgrounds. They examine the DOD's cyber supply chain risk management (C-SCRM), demonstrating the real risk and vulnerability implications, current processes, policies, and associated risk-mitigating efforts currently underway. This research offers the reader a hypothetical, scenario-based cyber-threat practical application exercise—identifying how special operators may become more resilient to cyber threats in their supply chain through awareness of potential adversary attack vectors across a product's life cycle—and concluding with their thoughts on the future of special operations acquisitions.

Advanced battlefield adaptations provide substantial force multipliers, and significantly contribute to improvements in force lethality, efficiency, and cost reductions. Across the military communications, command, and control's global connectedness of today's battlefield and tomorrow's hyper-enabled operator (HEO)—with thousands of networked weapons and communication devices, sensors, and streaming data all containing a multitude of diverse, complex, and commercially available hardware and software—there is an ever-expanding reliance placed on the cyberspace domain.

Through advances in communications technology, reductions in trade barriers, production and shipping costs, and an increase in international connections, the cyberspace vulnerabilities to military products and their supply chain have become progressively inherent in a product's life cycle. From concept to disposal, product interaction with precarious and often murky supply chain realities—consisting of multiple tiers of outsourced

contractors, subcontractors, manufacturers, and material suppliers that are increasingly diversified, fluid, and global—and the DOD's current acquisition strategies make it increasingly challenging to determine cyberspace risks in, or to, the delivered products.

Modern warfare has transformed into blended—physical and cyber—operations, and the supply chain is under increasing compromise by cyber threats. The stated compounding variables exponentially increase the potential exploitation of cyberspace product vulnerabilities by nefarious adversaries. This access may readily concede product security, integrity, and operating capability and have profound implications for mission success. Given the enormity and gravity of these challenges, how can the DOD and other federal entities protect and secure their cyberspace supply chain against adversary hacking, exploitation, disruption, or destruction?

As the authors adequately present, the notion of C-SCRM and resiliency is still a nascent and evolving concept; furthermore, they promote that C-SCRM is a distinct requirement originating from the U.S. government's acquisition strategy—pivoting from program-specific to commercial off-the-shelf products for missions and systems.

The emerging C-SCRM concept assists at all levels of the supply chain in managing and mitigating risks, and the authors define C-SCRM as the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information and operational technology products and service supply chains.

As Special Operations Forces increasingly rely on sophisticated hardware and software products, this quick, well-researched monograph provides a detailed accounting of C-SCRM associated laws, regulations, instructions, tools, and strategies meant to mitigate vulnerabilities and risks—and how we might best manage the evolving and ever-changing array of those vulnerabilities and risks.

Militaries will continue to evolve and seek out advanced software and hardware products, expanding their dependence on internet connectivity and cyberspace operations; therefore, we should expect everyone in the profession of arms to possess a basic understanding of C-SCRM. If the Cybersecurity Maturity Model, the Comprehensive National Cybersecurity Initiative, the Committee on National Security Systems, and the Cybersecurity & Acquisition Lifecycle Integration Tool are unfamiliar to the reader, this monograph will undoubtedly provide critical insights and lessons for those interested in

learning and subsequently contributing to this expanding and required field of study.

Mark Raney
Deputy Director, Institute for SOF Strategic Studies

About the Authors

Philip Craiger, Ph.D., CISSP, is a professor of cybersecurity in the Department of Security Studies and International Affairs. He currently serves as a co-principal investigator of the NSF-funded National Cybersecurity Training and Education Center (NCyTE). Philip previously served as professor in the School of Engineering Technology at Daytona State College, where he was the principal investigator of the NSF-funded Advanced Cyberforensics Education Consortium. From 2004–2010 he served a dual appointment at the University of Central Florida as the assistant director for Digital Evidence at the National Center for Forensic Science, and as an assistant professor in the Department of Engineering Technology. At UCF, Philip was instrumental in developing the first online Master of Science in Digital Forensics in the United States. Philip started his academic career as an associate professor in the Department of Computer Science at the University of Nebraska at Omaha. He is a member of the American Academy of Forensic Sciences and holds numerous professional cybersecurity certifications including Certified Information Systems Security Professional. Philip is a NAUI certified technical scuba instructor and instructor trainer, with hundreds of technical dives including cave dives in over 50 caves throughout the U.S. and Mexico, and several cave dives to 300 or more feet.

Laurie Lindamood-Craiger, M.S.M., is a contract specialist with Cubic Defense Applications, Inc. (the views expressed here are her own). Laurie received her master's degree in management with distinction from Embry-Riddle Aeronautical University, and a bachelor's degree from Texas Woman's University in government service. Prior to assuming her role in contracts, Laurie's background was primarily in instructional systems design and training delivery within the aviation security and defense sectors. Prior employers include The Boeing Company, the Transportation Security

Administration, and Lockheed Martin. Laurie is a member of the National Contracts Management Association and the National Defense Industry Association.

Dr. Diane Maye Zorri is an assistant professor of Security Studies at Embry-Riddle Aeronautical University in Daytona Beach, Florida and a non-resident senior fellow with Joint Special Operations University. Prior to Embry-Riddle, Dr. Zorri served as a visiting professor at John Cabot University, in Rome, Italy and as an affiliated scholar with George Mason's School for Conflict Analysis and Resolution. Prior to her work in academia, she was an officer in the United States Air Force and later worked in the defense industry doing foreign military sales, integrated communications, and proposal development for an Italian defense conglomerate. She is a graduate of the U.S. Air Force Academy, Naval Postgraduate School, and earned a Ph.D. in political science from George Mason University's Schar School of Policy and Government.

Introduction

Maersk is the world's largest container shipping company, with more than 800 seafaring vessels—many of which are enormous container ships, carrying millions of tons of cargo yearly throughout the world. Maersk accounts for a fifth of the entire world's shipping capacity.[1] In June 2017, a single internet-connected computer residing on Maersk's network became infected with a type of malware[2] called *ransomware*. Encryption effectively corrupts the computer's operating system and data files, rendering the computer inoperable until the files are decrypted, which returns the files to their original state. The ransomware spread quickly across Maersk's global information technology (IT) infrastructure, encrypting hard drives across 170 Maersk global offices, forcing recovery efforts to the entire IT infrastructure. Software and files were reinstalled on over 4,000 servers, 45,000 PCs, and 2,500 applications over a ten-day period.[3] The spreading mechanism embedded in the ransomware exploited two vulnerabilities in versions of the Microsoft Windows operating system. The first was a vulnerability in a Windows file sharing protocol that allows Windows-based computers to read and write files to and from other Windows-based computers on the same network. The second vulnerability was that some versions of Windows were known to leave users' passwords in the computer's working memory, and therefore potentially accessible to a technically inclined malign actor.[4] Once a single computer was infected, these vulnerabilities allowed the ransomware to automatically spread across Maersk's IT global infrastructure, infecting computers in other offices throughout the world.

The ransomware attack resulted in the incapacitation of Maersk's IT infrastructure; almost all office computers were inoperable, disrupting the company's ability to accept shipping orders and stranding millions of tons of freight in transit. Port terminals in the United States, India, Spain, and the Netherlands—all run by Maersk—experienced massive disruptions.[5] Although the computers on the cargo container ships were not affected, Maersk's office computers—most of which contained the logistics programs and information on their supply chain—were inoperable. Even when the container ships were able to dock at a port, the thousands of semi-trailer trucks that pick up and distribute cargo were unable to collect their cargo,

as there was no way of knowing which containers were on the ships or the cargo that was inside.[6]

The origin of this event was speculated to be a by-product of a state-on-state cyber offensive, part of the ongoing political conflict between Russia and Ukraine.[7] The ransomware was cleverly designed to automatically spread across a network when a single computer is infected. Unfortunately, the ransomware's spreading mechanism worked too well; it spread to computers on non-Ukrainian networks across the globe.[8] Several other global companies were affected by the ransomware, including the pharmaceutical company Merck, FedEx, the French construction company Saint-Gobain, snack company Mondelēz, and British manufacturer Reckitt Benckiser.[9] The U.S. government estimated that over $10 billion was lost due to the ransomware, and some have argued that figure was a conservative estimate.[10]

Of course, this does not tell the entire story of the effects of a 'glitch' in the supply chain. Clearly Maersk was affected, but also trucking companies, supply chain vendors waiting on the delivery of parts, distributors, and millions of customers and end-users. The intent of the malign actors was not to affect the supply chain, but the unintended side effects did just that. In the end it does not matter what the intent was, the effects on the supply chain were catastrophic.

As warfighting technologies have increasingly integrated information communications technology (ICT)—sophisticated hardware and software—there have been attendant changes in the worldwide supply chain.[11] The supply chain has transformed dramatically over the last few decades. Historically, the DOD mission needs could be met primarily through program-specific products—typically, custom designed and manufactured systems supplied by contractors. More recently and concurrent with advances in ICT, there has been a shift to commercial off-the-shelf (COTS) products and open source software where feasible and practical, as well as an increased reliance on non-U.S. suppliers via a "globalized market."[12] While these changes have led to significant improvements in efficiency and cost-effectiveness for the DOD, these changes have produced greater risks for DOD missions.[13] COTS products often rely on an even more complex and dynamic supply chain as smaller suppliers may change on an unpredictable basis. Custom weapons and support systems designed and built by contractors for specific mission needs most likely contain at least some COTS components (e.g., microelectronic components, software libraries, etc.), and, potentially, components

from non-U.S. suppliers. Accordingly, the DOD's current acquisition strategy presents the prospect of emerging threats in the supply chain through cyber compromise—either through intentional acts by malign actors, or unintentional acts by suppliers. Consequently, the government has pursued acquisition regulations and guidelines to assist in the mitigation and management of these threats. In this monograph, the authors describe the modernization of warfighting and the DOD's increasing reliance on ICT; the changing nature of supply chains and threats due to cyber compromise and their potential impact on SOF missions; and current as well as emergent government acquisition regulations and guidelines to mitigate and manage cyber supply chain threats.

Audience and Objectives

This monograph was written for a non-technical audience working with government acquisitions and procurement—including subcontractors, supply chain vendors, and risk managers. Additionally, decision makers in the supply chain—including those in acquisitions, cybersecurity, or IT—may find this monograph useful as it provides a context for the changing nature of supply chains; attendant cyber threats and risks; existing and emergent government guidelines and regulations affecting acquisition; and currently available tools to help mitigate risks for procurers and supply chain vendors.

The authors will use the following framework to address issues regarding supply chain threats and mitigation strategies, focusing on its effects on Special Operations Forces (SOF) mission readiness and capabilities:

Chapter 1. Characterizes the modernization of warfighting and increased use of ICT, and the attendant changes in supply chains;

Chapter 2. Introduces the subject of supply chains, threats, and threat mitigation strategies, including the notion of C-SCRM;

Chapter 3. Analyzes the supply chain from a SOF perspective—threats to the SOF supply chain, including historical threats and attacks on supply chains, as well as ramifications of cyber compromise in the supply chain;

Chapter 4. Describes existing government regulations, as well as emergent guidelines and regulations regarding government acquisition and procurement as a means of mitigating threats;

Chapter 5. Presents a hypothetical scenario of a warfighter as part of a larger system of smart, portable, and network-connected devices on the battlefield, and potential cyber threats at each stage of the life cycle of the warfighting systems;

Chapter 6. The authors discuss current SOF acquisition entities and practices, as well as other tools and emergent processes that can assist in securing the supply chain, as well as educating those involved in acquisition and procurement;

Conclusions. The authors then conclude with a discussion of the future of SOF acquisition.

The primary research question is: How can special operators become more resilient to cyber threats in their supply chain? To answer this question, the authors' research addresses threats to the cyber-resilience of the supply chain, the potential effects of cyber compromise on the warfighter, and how SOF can mitigate threats to their supply chain. To examine future uncertainties, the authors include a hypothetical scenario-based case study featuring the future, hyper-enabled warfighter as part of an integrated system comprised of smart, portable, network-connected technologies, addressing cyber threats at each stage of the system life cycle. This method allows the researcher to create plausible future scenarios based on a process-tracing of current technological trends, thereby showing a series of alternative potential events. Because technology changes so rapidly, the scenario-based case study methodology provides a logical framework for researching not only the threats and vulnerabilities, but also mitigation strategies.

Definitions

Although this monograph was written for a non-technical audience, to provide accurate descriptions of cyber threats requires the use of cyber-related terminology—some of which may be foreign to readers—yet likely to be encountered for those working in acquisition and procurement as government guidelines and regulations emerge to mitigate cyber threats. The authors provide, in the following, brief definitions of this terminology. These definitions level the bubble, making sure that everyone understands the terms used.

Cybersecurity: The process of protecting information and information systems by preventing, detecting, and responding to attacks. The objective is to reduce the likelihood that attackers can access DOD systems and limit the damage if they do.[14]

Vulnerability: A weakness in a system that could be exploited to gain access or otherwise affect the system's *confidentiality*, *integrity*, and *availability*.[15] *Confidentiality* involves limiting system and information access to authorized users and for authorized purposes only; *integrity* involves ensuring information and systems are not modified by unauthorized users and that the systems function as designed; and *availability* involves ensuring information and services are available to authorized users when needed.[16]

Threat: Anything that can exploit a vulnerability to damage or impede a system, either intentionally or unintentionally.[17]

Attack vector: The path or means by which a malign actor exploits a vulnerability. Sometimes used synonymously with the term "threat vector."

Exploit: A method of attack that takes advantage of a vulnerability in a system.

Cybersecurity risk: A function of the threat (intent and capabilities of the malign actor), vulnerabilities (inherent or introduced), and consequences (fixable or fatal).[18] The extent to which a malign actor has the intent and capabilities, combined with existing vulnerabilities and consequences, will determine the amount of risk involved.

C-SCRM: The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/operational technology (OT) product and service supply chains. It covers the entire life cycle of a system—including design, development, distribution, deployment, acquisition, maintenance, and destruction—as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.[19]

Cyber resiliency: Involves identifying and protecting critical system elements during a cyberattack to ensure that they can continue to operate, possibly with limited capabilities.[20]

Chapter 1. Modern Warfighting Technologies and the Supply Chain Problem

U.S. SOF are facing unprecedented changes to their operating environment as sophisticated computer hardware and software have become increasingly important as force multipliers for SOF's warfighting capabilities. These technologies provide warfighters with enhanced resources surpassing technology of old; for instance, SOF's fully integrated panoramic night-vision goggles have no analogue technology from the Vietnam War. Likewise, portable and lightweight communication systems permit satellite communications to warfighters in the field—a profound evolution from previous communications technologies. More recently, smart and portable network-connected devices are increasingly deployed by the DOD. These devices have robust applications that support information flow between warfighters, aircraft, naval vessels, unmanned aerial systems, and command posts, forming a unified network that increases situational awareness, response time, and risk assessment.[21]

The Chief Scientist of the U.S. Army Research Lab coined the term Internet of Battlefield Things (IoBT) for smart, portable, network-connected devices that will transform the future of warfighting:[22]

> In the future, military operations will rely less on human soldiers and more on interconnected technology, leveraging advancements in unmanned systems and machine intelligence to achieve superior defense capabilities. The IoBT (Internet of Battlefield Things) will connect soldiers with smart technology in armor, radios, weapons, and other objects, to give troops "extra sensory" perception, offer situational understanding, endow fighters with prediction powers, provide better risk assessment, and develop shared intuitions.[23]

An early instance of IoBT involved U.S. Army helmets containing built-in sensors that transmitted sensed health data to physicians over networks to assist in diagnosing brain injuries.[24] IoBT are increasingly deployed on the battlefield, and their role will continue to expand in future warfighting.[25]

Current and emergent warfighting technologies are composed of significantly more diverse, complex, and commercially available hardware components and software than any time in military history.[26] The supply chain for these technologies may involve sourcing from a hierarchy of suppliers—from prime contractors, to Tier 1 through 4 subcontractors that provide hardware components, software, and services to upstream and downstream suppliers within the supply chain. Even lower tier suppliers, often small- and medium-sized businesses, are reliant on a global supply chain network.

Figure 1 is an illustrative yet oversimplified example of the complexities of the global supply chain.[27]

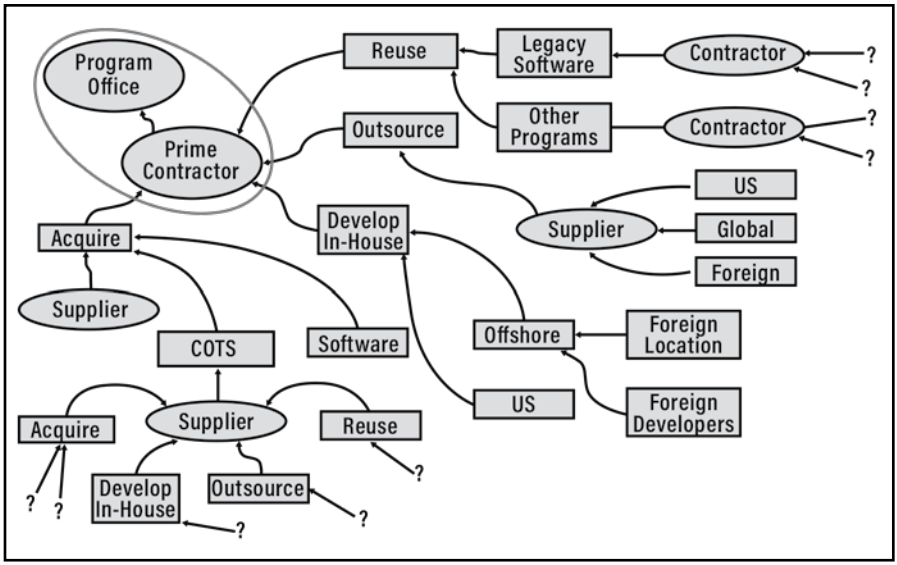

Figure 1. 21st Century Global Supply Chain. Derivative from *Insight* article created by authors.

As depicted in figure 1, the source of hardware components or software may not be evident to other participants within the supply chain. For example, a procurer (e.g., Program Office) may only be able to identify the sources to which it is directly connected in the supply chain.[28] Additionally, the intricacy of corporate structures can obfuscate the identity of downstream suppliers, such as when parent companies and their subsidiaries control businesses using different names in multiple countries, which further obscures the provenance of products.[29] As such, the procurer may have little knowledge of its downstream suppliers. Knowing the suppliers of your suppliers

can be daunting: in 2017, U.S. defense contractor Raytheon was estimated to have 36,000 suppliers alone, and about 65 percent of those were also suppliers for other major contractors such as Boeing, Lockheed Martin, and Northrop Grumman.[30] The supply chain problem is further complicated when suppliers change on a unpredictable basis, such as when suppliers are acquired by or merged with another supplier—not unheard of for small- and medium-sized businesses—further obfuscating provenance.

The difficulty of identifying the participants in the DOD supply chain results in the futility of not only identifying the provenance of hardware and software, but adherence by suppliers to DOD acquisition standards and regulations as well:

> DOD systems are exposed to threats of malicious insertion and tampering throughout the development and supply of critical components from external and internal sources. This exposure is further exacerbated by the use of a significant number of COTS parts that are obtained through a global supply chain. Examples of malicious insertion threats are widely publicized and include telecommunication switches that exfiltrate data and radar systems that are unable to detect a particular country's planes.[31]

Figure 2 displays the stages in the life cycle of a "product," whether a hardware component, software, or an integrated system.[32] Due to the complexity of modern weapons systems, there may be many participants involved in the supply chain, exposing opportunities for cyber compromise.[33] Between the inception of a component or a system and its final disposal, there are several stages in the life cycle where it can be altered, moved, shipped, tested, packaged, sold, used, and maintained. Likewise, components and systems can encounter several different handlers, engineers, testers, logisticians, consumers, owners, and users during their life cycle. At each of these stages of the life cycle, there are opportunities for malign actors to interfere with the integrity of components or the systems themselves for malicious purposes.

Figure 2. Supply Chain Product Life Cycle. Graphic created from data in *Sandia Report* by authors.

Given the ubiquity and reliance on ICT in operational environments, support, suppliers, and supply chains are under constant and increasing threat of cyber compromise. State-of-the-art integrated weapons and support systems employed by SOF warfighters could potentially contain cyber vulnerabilities—in hardware and/or software—and therefore require new risk mitigation strategies.[34] The National Institute of Standards and Technology (NIST)[35] noted that cyber supply chain risks include insertion of counterfeit components,[36] unauthorized production,[37] tampering,[38] theft,[39] insertion of malicious software[40] and hardware,[41] and poor manufacturing and development practices in the supply chain.[42] The DOD has acknowledged issues with its supply chain in the last decade, where it was estimated that 15 percent of spare and replacement parts have been identified as counterfeit.[43] Counterfeit electronic parts have been identified on U.S. Navy SH-60B helicopters, U.S. Air Force C-130J, U.S. Coast Guard C-27J cargo planes, and the U.S. Navy P-8A Poseidon aircraft.[44]

The effects of a cyber supply chain vulnerability are not confined to the DOD; vulnerabilities can pass to federal agencies, enabling malign actors to exfiltrate data, insert malicious content, or otherwise exploit these vulnerabilities, potentially resulting in the compromise of federal information or missions.[45] In response to threats to the cyber supply chain, the concept of C-SCRM emerged to assist all tiers of the supply chain in managing and mitigating risks. The DOD established additional requirements for contractors which store, process, or transmit covered defense information and implemented the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204.7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.[46] This clause was implemented by a rule released in December 2015 which mandated compliance by contractors. The clause required contractors and subcontractors to implement NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*,[47] which lists 110 security controls with which suppliers must be compliant, as well as implementing new rules regarding cyber incident reporting. Contractors risk losing their current federal contracts, and are potentially barred from future contracts for noncompliance.[48]

In 2014, the NIST released *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.0, and a revised Version 1.1 in 2018, referred to as the "Framework."[49] Although the Framework was designed to be voluntary,

it provides a method for organizations to measure and manage risks. Version 1.1 implemented C-SCRM considerations and identified risks specific to the supply chain, as well as subcontracted parts and materials.

The notion of C-SCRM and resiliency is still a nascent and evolving concept as supply chains become more complex, fluid, unpredictable, and globalized. In January 2020, the Undersecretary of Defense for Acquisition and Sustainment emphasized the supply chain risk when she stated: "[a]dversaries know that in today's great power competition environment, information and technology are both key cornerstones … and attacking a sub-tier supplier is far more appealing than a prime."[50] While the DFARS mandates compliance, many lower-tier suppliers—often small- to medium-sized businesses—may be incapable of managing and meeting the requirements imposed by these regulations, in contrast to large, long-established, and therefore ostensibly more robust suppliers (e.g., Lockheed, Boeing, Raytheon, BAE Systems, General Dynamics, Northrop Grumman, etc.).[51] But because of the risks inherent in the supply-chain, even these latter suppliers are not immune to cyber compromise.[52]

The notion of C-SCRM and resiliency is still a nascent and evolving concept as supply chains become more complex, fluid, unpredictable, and globalized.

In 2017, The Defense Science Board (DSB) Task Force report *Cyber Supply Chain* noted the warfighters' increasing reliance on sophisticated ICT-based weapons systems, and potential problems with the supply chain:

> Modern weapons systems have depended on microelectronics since the inception of integrated circuits over fifty years ago. Today, most electronics contain programmable components of ever-increasing complexity. At the same time, the Department of Defense (DoD) has become a far less influential buyer in a vast, globalized supplier base. Consequently, assuring that defense electronics are free from vulnerabilities is a daunting task.[53]

As in the past, weapon systems will continue to leverage the latest technologies. Modernization requires increases in system complexity, meaning more physical hardware components and more complex components.[54] But system complexity is not only defined by the number of physical hardware

components or their complexity; equally important is the software that defines the system's functionality:

> For many if not most DOD systems, software now defines function. Software increasingly determines the boundaries, operation, and risks to systems relied upon by all facets of civil society—consumer-facing, industrial, transportation, energy, healthcare, communications—as well as defense missions and management. Increasingly, functionality is achieved through software. A modern aircraft may have more than 10 million lines of code. The initial Block 1A/1B F-35 had more than 8.3 million lines of code, and later version of the aircraft will have more than 20 million lines of code for both operations and support. Combat systems of all types increasingly employ sensors, actuators, and software-activated control devices.[55]

Software is the computer instructions that connects weapon system's components, subsystems, and sensors.[56] Some hardware components may be designed for specific uses—e.g., microelectronics for a specialized heads-up display. Other hardware are general purpose systems—e.g., COTS laptop computers, smartphones, etc.—which might be composed of specific-use components. Nonetheless, hardware systems cannot function unless software is written to make use of the hardware's capabilities.

Modernization introduces complexity into weapons systems in terms of the number and complexity of hardware components, lines of software code, as well as the complexity of the code. In concert, the supply chain for hardware and software is increasingly diversified, fluid, and global. Consequently, there is concurrent increase in the *attack surface* for weapons and support systems, meaning more and varied opportunities for malign actors to attack the systems through hardware and/or software, through multiple channels in the supply chain, and through all stages of a system's life cycle shown in figure 2.[57]

Chapter 2. Supply Chains, Threats, and Mitigation Strategies

For the purposes of this research, when describing supply chain and supply chain management (SCM), the authors use a widely cited definition proposed by Mentzer, DeWitt, Keebler, Min, Nix, Smith, and Zacharia in the *Journal of Business Logistics*.[58] They defined the supply chain as a "set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer."[59] Meanwhile, they define SCM as:

> The systemic, strategic coordination of the traditional business functions and the tactics across these business functions within a particular company and across businesses within the supply chain, for the purposes of improving the long-term performance of the individual companies and the supply chain as a whole.[60]

Increases in the use of non-U.S. suppliers via a globalized market, and the rise of ICT, has triggered rapid changes in the way businesses operate within their supply chains.[61] Virtual distance reduction, interactivity, disintermediation among supply chain participants, and the development of new businesses—especially around digital product using the internet—has significantly affected SCM. Additionally, an increasing reliance on the Internet of Things (IoT), small network connected computing devices—which are covered in depth later in this monograph—have allowed for increasing integration within supply chains of processes, people, and things.[62] Modern supply chains include contractors, suppliers, manufacturers, trading firms, and transport firms that work in tandem in online networks, blurring the lines between organizations.[63] Geographic networks are now more diverse, with more suppliers involved, and these supply chains move both tangible and intangible assets—which can be prone to disruption.[64] Accordingly, operations structures are needed to manage risks including reputational, intellectual property, and liability to maintain continuity of supplies.[65] The Government Accountability Office (GAO) noted the complexity and challenges of the federal ICT and communications supply chain:

> Federal information and communications systems can include a multitude of IT equipment, products, and services, each of which may rely on one or more supply chains. These supply chains can be long, complex, and globally distributed and can consist of multiple tiers of outsourcing. As a result, agencies may have little visibility into, understanding of, or control over how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services.[66]

The conclusion can be drawn that disruption to the stability of the supply chain can lead to undesirable consequences to the operational readiness of DOD services—and more specifically, to SOF—because the more critical a product is to mission success, the greater the consequences for any disruptions in the end-to-end supply chain, resulting in second and third-order effects on mission outcomes.[67]

The very benefits of the global interconnected supply chain—rapid innovation, interoperability, low-cost, and product features—are the very things that leave it vulnerable to supply chain compromises, whether intentional or unintentional.[68] To properly manage the supply chain, it is necessary for participants in the supply chain to ensure the quality, integrity, security, and resilience of supply chain services and products to prevent the introduction of cyber supply chain risks such as unauthorized production, theft, insertion of counterfeits, tampering, introduction of malicious hardware and software—and the risks presented when firms in the cyber supply chain have poor development and manufacturing practices.[69]

The very benefits of the global interconnected supply chain—rapid innovation, interoperability, low-cost, and product features—are the very things that leave it vulnerable to supply chain compromises, whether intentional or unintentional.

As the supply chain underwent major transformations with the emergence and evolution of ICT, initial concerns regarding cyber security at the federal level began surfacing in the 1990s—specifically, how U.S. national security interests could be damaged due to the use of the internet and telecommunication systems.[70] The electronic information systems supported a wide range of activities, both in the private and public sectors, and these

information infrastructures supported a wide variety of economic and security assets.[71]

In 2013, C-SCRM was identified as a distinct need due to changes in the U.S. government's acquisition strategy, with the government pivoting from program-specific products to COTS products for missions and systems.[72] This fact, combined with increased access to non-U.S. supply chain sources, provided the U.S. government an opportunity to buy the best products at lower prices.[73] However, as the global ICT supply chain became more interconnected, it introduced the risk of malign actors exploiting these systems.[74] While the COTS acquisition strategy lowered costs, the reduced visibility and control throughout the life cycle of the supply chain led to an increased risk of compromised components which could have malicious elements, be counterfeit, or be flawed in some other way.[75] The DOD's increasing reliance on ICT could lead to system vulnerabilities, allowing information such as inventory or troop strength to be accessed by a malign actor—which could, for example, negatively impact SOF mission outcomes.[76] How then to best manage this evolving and ever-changing risk?

C-SCRM

C-SCRM is an emerging area of both research and practice, and joins SCM, risk management, and cybersecurity, incorporating practices from these fields to manage the risks associated with the global interconnected supply chain. In response to the Comprehensive National Cybersecurity Initiative (CNCI) *#11*—which addressed C-SCRM for non-national security information systems—NIST developed C-SCRM best practices with input from academia, industry, and government.

The CNCI was established under President George W. Bush in January 2008, by the *National Security Presidential Directive 54/Homeland Security Presidential Directive 23* (*NSPD-D54/HSPD-23*), but was kept confidential at the time.[77] The CNCI flowed from the 2003 Bush administration National Strategy for Security Cyberspace policy, which recognized the existence of cyber threats, and the need for a coordinated national response.[78] The administration established the CNCI to better protect agency networks from malign actors such a foreign nation state, as well as from non-state technical malign actors.[79] The CNCI also worked to unify fragmented federal agencies response to reduce the risks of threats to government networks.[80]

At the time, the CNCI consisted of 12 components to improve the government's cybersecurity by formalizing existing procedures and introduce new business practices and policies to better protect government networks.[81] Limited information emerged that one of the components of the CNCI was to address the risk of malicious hardware and software that could be inserted into a product or into a contractor's network to allow malign actors a view into the government's data.[82]

In March 2010, President Barack Obama released a sanitized version of the CNCI that was subsequently published on the White House's website.[83] One of the CNCI's core goals was "to defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies."[84] *CNCI #11* specifically identified the risk that globalization of the ICT presented opportunities for malign actors to use the supply chain to gain access to data, interrupt communications, or alter data.[85] Furthermore, the CNCI acknowledged that the global supply chain must be managed over the entire life cycle of services, products, and systems in comprehensive and strategic ways—and that managing this risk required greater attention to vulnerabilities, threats, and consequences of acquisition decisions.[86] *CNCI #11* also called for the development and use of resources and tools to mitigate risk both technically and operationally across product life cycles from design to retirement.[87] The CNCI also recognized the importance of the acquisitions, calling for new policies and practices that mirror the global market place complexities.[88]

Concurrent with the government's recognition of the need for C-SCRM, there were growing calls for increased attention and research on C-SCRM. There was a general recognition that C-SCRM was not widely understood by academia or industry, and while C-SCRM was rapidly evolving, it was still a nascent area of risk management research. While C-SCRM has its roots in ICT management, there was growing recognition that risks expand beyond ICT systems, requiring a merging of perspectives within the C-SCRM discipline. Academics recognized that C-SCRM bridged multiple disciplines and practices: "[t]he cybersecurity problem does not fit conventional or traditional security categories based on individual security responsibilities, economic or corporate security issues, military security problems, as well as domestic versus international problems."[89]

The academic literature has provided C-SCRM models that have evolved over time, and it is helpful to review the literature to understand how current definitions of C-SCRM were derived. As early as 2010, collaborative efforts between industry, academia, and government resulted in an early risk management framework (RMF) to address risks within the electronics supply chain.[90] The framework created a typology for the four types of risks and mitigation strategies within the electronics supply chain:

1. If a firm is attacked by malign actors, the firm's operational capabilities may be at risk.
2. If malign actors can infect computer systems with malware, a firm's operation and its data can be compromised.
3. In the event of an attack, the reputation of a firm and the trustworthiness of the firm are both at risk.
4. The existence of the firm itself is at stake if there is a loss of control or competitive information.

Several strategies have been offered to address supply chain risks.[91] First, production should be mandatory and continual with alternate production sources maintained to ensure continuity within the supply chain and avoid the interruption of operations.[92] Second, strict controls should be used to guard against malware threats and the associated risks of corruption to intellectual property.[93] Third, seals should be used on electronic products, and containers should be tracked and sealed as well to prevent tampering. Fourth, operational logs should be implemented to assist in identifying responsible parties to help maintain trust.[94] Finally, versioning control can be used to prevent loss of information and intellectual property.[95] The strategies used to manage risks relate various stages in the supply chain including design, fabrication, assembly, and distribution. While simple, this was an early approach to addressing and managing emerging supply chain risks.

Other researchers expanded beyond electronics products and focused on the risks associated with enterprise SCM information systems—focusing on the early IT implementation of these systems—and noting that interruptions to these systems could cause business losses.[96] For example, a "lessons learned" approach was used to create a RMF that integrated elements from IT, supply chain, and risk management, and further identified the need for

information confidentiality, integrity, and authenticity.[97] Due to its narrow focus on implementation, this framework did not address life cycle C-SCRM.

Other research in this field used risk mitigation factors to determine and assess threats.[98] For instance, product criticality should be considered because risks introduced in the end-to-end global supply chain can have an impact on mission success.[99] Threats and vulnerabilities should be identified and prioritized, and countermeasures to mitigate risks identified.[100] Then firms can identify how best to allocate resources for risk mitigation using a return-on-investment approach.

Given the increasing diffusion of software and hardware systems in the supply chain, some have argued for a need to view C-SCRM as a blended discipline.[101] Within a company, IT department goals—such as cutting costs—may be at odds with other organizational goals, and structural integration of the supply chain does not occur.[102] Consequently, C-SCRM should combine not only SCM and cybersecurity, but also incorporate enterprise-level risk management practices.[103]

Nuances exist between the terms IT, cybersecurity, SCM, and C-SCRM.[104] C-SCRM expands IT's role beyond the firm itself, to include Tier 1 and Tier 2 partners in the supply chain in order to provide greater control and insight.[105] Cybersecurity focuses on finding technical solutions for cyber threats, whereas C-SCRM also considers broader supply chain disruptions and integrates broader perspectives such as human factors and management.[106] Enterprise risk management typically focuses on the top-down control of the business's environment, and C-SCRM redirects this focus to include the sometimes hidden, but adaptive dynamic and global supply chain.[107]

Cybersecurity focuses on finding technical solutions for cyber threats, whereas C-SCRM also considers broader supply chain disruptions and integrates broader perspectives such as human factors and management.

In 2011, the notion of a research-based capability/maturity model for C-SCRM emerged.[108] The federal government created a focus group of 19 participants, including the Federal Communications Commission (FCC), Department of Homeland Security (DHS), National Security Agency (NSA), the DOD, and major suppliers to discuss the inception of a C-SCRM capability/maturity model.[109] The focus group's findings were combined with other research to create a cyber supply chain framework. Subsequently, the

government studied sixty public and private-sector organizations to evaluate the effectiveness of these organization's C-SCRM standards and policy initiatives in addressing end-to-end supply chain risks.[110] The organizations' initiatives were reviewed to determine how much they addressed each tier's key attributes using a three-tiered framework, which considered systems integration, governance, and operations.[111] The research findings suggested that the organizations' C-SCRM supplier-sourcing activities were found only for key suppliers, meaning that organizations had little visibility or knowledge of downstream suppliers.[112]

The focus group then created a C-SCRM capability/maturity model that identified and classified practices as *average*, *more advanced*, or *leading edge*, and then linked to the system integration, governance, and operations tiers.[113] The model acknowledged that C-SCRM practices and performance could then be categorized as *emergent*, *diligent*, and *proficient* in regard to the status of the implementation of C-SCRM practices, and accordingly, if practices were not implemented, but were planned, the organization would be considered emergent.[114] If an organization was in the early stages of implementation with ongoing implementation efforts, the organization would be considered diligent. Organizations rated proficient would have process improvements across the supply chain, and the implementation would be well-established.[115]

Others observed that while IT has the capability to maximize SCM, it also opens organizations to vulnerabilities that can be exploited by malign actors and therefore require cyber resilience strategies.[116] This approach had a narrower technical focus to managing cyber supply chain risks, focusing on IT-based platforms to address cyber supply chain risks and maintaining cyber resilience using cost-effective, push/pull services.[117] It was advocated that all parties—both industry and government—have data access in the supply chain that is common and reliable.[118] Pull services provide a way for a supply chain organization to evaluate supply chain elements such as inventory levels of a supplier, shipment location, or even traffic conditions using data pulled from integrated systems and are more suitable for managing their supply chains.[119] Push services permit organizations to send alerts such inventory level or demand if unanticipated changes occur and address risk and supply chain resiliency.[120]

Academics also investigated the idea of managing C-SCRM using an IT systems engineering approach.[121] Firms across the supply chain, including end-user organizations such as SOF, may have different understandings of

risk management objectives and different abilities to define and manage cyber supply chain risks.[122] Organizations within the supply chain may be motivated by differing risks tolerances and appetites, and therefore make trade-offs in C-SCRM accordingly, without considering other parts of the supply chain.[123] To address this issue, C-SCRM stakeholders introduced systems engineering concepts into the management of cyber supply chain risks, including security, safety, reliability, trustworthiness, and quality.[124]

Some have made the case that C-SCRM must include additional functions beyond IT due to the multiple potential failure points in the supply chain.[125] These areas include supply chain continuity from product sourcing, management of suppliers, security, quality, and transportation. Additional functional management areas needed to manage cyber requirements include human resources, strategy governance and controls, processes and standards, regulation and law, research and development (R&D), supplier management, manufacturing, verification, audit, defects, secure delivery of services, and vulnerability resolution.[126]

Other researchers recommended a tiered maturity/capability model to manage cyber supply chain risks, but expanded the organization's activity to downstream suppliers, consumers, and organizations.[127] In this approach, ad-hoc risk management characterizes Tier I as initial organizations, and these organizations partially follow C-SCRM practices.[128] Management approval of C-SCRM practices characterize Tier II as managed organizations—but operationally, implementation of these practices may not occur and there is not repeatable risk assessment.[129] As with Tier II, organizations with approved management practice characterize Tier III as defined organizations, but at this tier, repeatable risk assessment occurs and agreements and communications with the government, suppliers, and consumers have been established.[130] Organizational implementation of the highest level of C-SCRM practices characterizes Tier IV as optimizing organizations, with continuous process improvement occurring as well.[131] Further, at this level real-time risk management occurs, and there is coordination of C-SCRM with other consumers, suppliers, and organizations.[132]

Some researchers examined C-SCRM from the perspective of operations and supply chain management and the challenges of preserving digital confidentiality.[133] With greater systems integration comes a need for organizations to understand the risks they face with this integration.[134] Accordingly, C-SCRM is seen as not just an activity that occurs within IT, but as something that also needs to be incorporated in all business operations daily. The ability to maintain digital confidentiality increasingly drives a firm's viability and reputation—however,

maintaining digital confidentiality can be in tension with increased system integration.[135] The Occupational Classification System Manual literature identifies high levels of digital integration among organizations within the supply chain but does not consider the attendant risks this creates for firms trying to maintain digital confidentiality, presenting a dichotomy between supply chain practice and the literature.[136]

Other researchers identified IT supply chain risks as micro risk within a larger supply chain risk management (SCRM) framework.[137] Macro risks for SCRM are relatively rare events, e.g., earthquakes or war, while micro risks refer to the relatively routine activities that occur within an organization or its business partners.[138] Both macro and micro risks—including IT disruptions—should be managed in a continuous manner.[139] A four-phase approach was proposed to manage cyber supply chain risk: identification, assessment, mitigation, and monitoring.[140]

The Federal Information Security Modernization Act of 2014 required NIST to provide agencies with the standards and guidelines needed to improve information security.[141] As a result, NIST has taken a lead role for the federal government in consolidating a definition of C-SCRM—by taking a multi-disciplinary approach to defining cyber terminology, and recommending strategies to deal with cyber risks using input from government, industry, and academia.[142]

While NIST provides a suitable definition of C-SCRM, the GAO noted that additional supply chain vulnerabilities can occur in "agency acquisition or security procedures, controls, or implementation related to an information system."[143] These vulnerabilities provide opportunities for malign actors to exploit the supply chain. The GAO identified three categories of vulnerabilities in IT acquisitions: (1) gray markets, (2) distributors, and (3) independent brokers who are not the original equipment manufacturer (OEM) or an authorized reseller; those three categories are all present risks in IT acquisitions. Another category of vulnerability exists in software updates and patches that have been inadequately tested. Finally, the GAO acknowledged that there may be inadequate information on suppliers of IT systems. These supply chain vulnerabilities, if compromised, present risks to end users such as SOF, a point made by the GAO:

> If a threat actor exploits an existing vulnerability, it could lead to the loss of the confidentiality, integrity, or availability of the system and associated information. This, in turn, can adversely affect an agency's ability to carry out its mission.[144]

Chapter 3. The SOF Supply Chain Problem

SOF weapons and support systems procurement relies on a complex, dynamic, and sometimes unpredictable supply chain, with multiple tiers of vendors supplying hardware, software, and services to upstream suppliers and prime contractors in a complex chain of relationships. The life cycle of a SOF weapons system can be years-long, from the initial concept and design, to manufacture, deployment, maintenance, and at the end, disposal. Each life cycle stage presents additional opportunities for cyber compromise. Cyber compromise need not be *intentional* acts by malign actors. Unintentional acts by suppliers, such as lack of due diligence, or inferior design, manufacturing, and system testing practices, can also result in vulnerabilities and system compromise. Regardless of intent, vulnerabilities must be identified, addressed, and mitigated.

Unintentional acts by suppliers, such as lack of due diligence, or inferior design, manufacturing, and system testing practices, can also result in vulnerabilities and system compromise.

Vulnerabilities may be persistent and not apparent even after rigorous testing of hardware components and software. For instance, software development requires testing to confirm that software supports the functionality specified in the requirements and design stages. Unless the source code has been thoroughly reviewed by programmers or software engineers, what is not apparent is the answer to the question "what else does the software do?" It is difficult to identify hidden functionality in compiled code,[145] and this hidden functionality may "execute" under certain specific conditions or a set time. For example, in 2002 a disgruntled employee successfully deployed a logic bomb against UBS PaineWebber, his employer, after a dispute over his annual bonus.[146] The employee installed the logic bomb on 2,000 computers across 400 offices, and set it to execute on 4 March 2002, at 9:30 a.m., whereupon it would delete files on UBS servers and backup systems. On the appointed date and time, the logic bomb executed, leaving over 17,000 brokers unable to make trades.[147] From a DOD perspective, persistent, latent vulnerabilities can lead to mission failure in modern weapons systems, and the cause may be difficult to distinguish from normal electronic or mechanical failure.[148]

Hardware must also be subjected to testing, yet, it has the same issues as software in terms of the potential for persistent, undetected vulnerabilities. Even after extensive testing, vulnerabilities may not be identified until years later. For example, in March 2020 a team of academics identified vulnerabilities in AMD Central Processing Units (CPUs)[149] that were sold from 2011 to 2019.[150] The vulnerabilities could theoretically allow a malign actor to exfiltrate information from the CPU. CPUs from another major manufacturer, Intel, were also found to contain two similar vulnerabilities, one of which dated back to 1995.[151] As discussed later, identifying cyber vulnerabilities with hardware is just as difficult as with software, and presents a malign actor with opportunities for cyber compromise.

The nature of modern warfare has changed dramatically because of evolving and emergent ICT-based technologies.[152] No longer are adversaries engaging the U.S. solely via kinetic means; they have moved to asymmetric warfare with "blended operations that take place through the supply chain, cyber domain, and human elements."[153] Malign actors can and do use multiple attack vectors to trigger operational effects, thereby increasing the potential for mission disruption. Four primary attack vectors used in asymmetric blended operations include:[154]

- supply chain attacks through hardware, software, or services
- cyber-physical system (CPS) attacks through weapons systems or industrial control systems
- cyber IT attacks through IT
- human domain attacks through insiders, foreign intelligence services, or witting/unwitting actors

Although the preceding list of attack vectors separates supply chain as its own category, the three remaining attack vectors can also play a part within the supply chain, and therefore will be addressed accordingly. The human domain is also divided into several subcategories, given that there are multiple critical attack vectors within that category. The following discusses each attack vector and provide descriptions of potential cyber threats as well as historical examples of attacks.

Supply Chain Attack Vector

As noted earlier, each stage of the product life cycle presents new opportunities for cyber compromise by a malign actor—such as inserting a

vulnerability or malicious functionality—or unintentional acts by insiders as the result of poor design, manufacturing, and/or testing practices by suppliers. Regarding the former, consider a hardware implant inserted into microelectronics by a malign actor during the manufacturing stage. A hardware implant is an extra component that is manufactured into microelectronics that provides functionality not specified in the requirements or design stages. This extra component might, for instance, allow a malign actor to gain unauthorized access to a weapon or support system through a backdoor, permitting the actor to access, add, modify, or delete critical functionality or data stored on the device.[155]

In 2018, *Bloomberg Business* reported on the result of over a yearlong investigation into a hardware implant allegedly traced to China.[156] The implant involved a supply chain attack by the Chinese motherboard[157] manufacturing company Supermicro, Inc.[158] The story starts in 2015 when Amazon considered acquiring Elemental, a company that develops and sells hardware and software for compressing large video files. Elemental's video compression servers at the time were assembled by Supermicro, one of the largest motherboard suppliers in the world, with Elemental being only one of hundreds of Supermicro customers. Although Supermicro had several production facilities throughout the world, including California, Taiwan, and the Netherlands, Chinese contractors manufactured their motherboards.

In 2015, Elemental shipped several of these servers for testing to an independent third-party cybersecurity company. The security company identified a small microchip, no larger than a grain of sand, that was not a part of the motherboard's original design specification. The finding was reported to U.S. governmental authorities, causing alarm as the motherboards had been purchased by numerous commercial and government entities. Particularly concerning was that the motherboards were deployed on U.S. Navy warships, as well as within the Central Intelligence Agency's (CIA) drone operations. This finding started a multi-year classified government investigation into Supermicro and its motherboards.

The government conducted further testing to identify the chip's functionality. The chip was connected to the baseboard management controllers, which are tiny computing devices connected to servers to provide computer administrators remote access to the device to troubleshoot or restart the system remotely. Given its location, it was surmised that the microchip served as a backdoor to the systems on which the motherboard was installed.

Sources not identified by *Bloomberg* further asserted that the implants had been installed during the manufacturing process by operatives from the Chinese People's Liberation Army.

The investigation identified 30 companies that had purchased the contaminated motherboards, including Apple Inc., a major bank, and several government contractors. As reported by *Bloomberg*, further research by Apple Inc. confirmed the hardware implants on the motherboards purchased from Supermicro, and in 2015, Apple severed ties with Supermicro. Supermicro denied all allegations. Some security researchers expressed doubts about the allegations regarding the functionality of the implant as unnecessarily complex, cumbersome, and easily accomplished with software or firmware instead.[159,160] Meanwhile, others have expressed skepticism at the *Bloomberg* report, including the NSA.[161]

CPS Attack Vector

CPS are smart systems that include interacting networks of physical and computational components.[162] ICT-based modern weapons systems are prime examples of CPS. A 2018 GAO report described persistent and ongoing problems with DOD weapons system's cybersecurity:

> Multiple factors contribute to the current state of DOD weapon systems cybersecurity, including: the increasingly computerized and networked nature of DOD weapons, DOD's past failure to prioritize weapon systems cybersecurity, and DOD's nascent understanding of how best to develop more cyber secure weapon systems. Specifically, DOD weapon systems are more software and IT dependent and more networked than ever before. This has transformed weapon capabilities and is a fundamental enabler of the United States' modern military capabilities. Yet this change has come at a cost. More weapon components can now be attacked using cyber capabilities. Furthermore, networks can be used as a pathway to attack other systems.[163]

The GAO report noted that from 2012 to 2017, DOD security testers routinely identified critical cyber vulnerabilities in almost all of the weapon systems under development.[164] The testers used well-known penetration testing techniques and easily obtainable penetration testing tools.[165] The testers

seized control of these systems and were able to largely remain undetected by the system's operators. When a system operator identified an intrusion, in some cases, the operator was unable to effectively respond to the intrusion. The report noted that a two-person team gained initial access to a weapons system in under an hour, and in a day the team was able to escalate privileges to take full control of the weapons system.[166] After escalating privileges, testers were able to move through the system unimpeded and unnoticed. In one instance testers were able to view in real-time what the operators were viewing on their console and could manipulate the system's controls. Additionally, multiple penetration testing teams were able to copy, modify, or delete system data—including one team that downloaded over 100 gigabyte (GB) of data. Perhaps most disturbing, one team noted that performing a simple passive scan caused a weapons system to shut down.[167] Another team reported they were able to guess the system's administrator password in nine seconds. Some of the weapons systems incorporated COTS and open-source software that had not been reconfigured with new passwords to replace default passwords shipped with the system. This allowed testers to search the internet to identify the default passwords, which the testers subsequently used to gain access and control the systems.

Note that the DOD cybersecurity testers were conducting "friendly" cybersecurity tests in this case, causing no actual damage. Moreover, these vulnerabilities were not alleged to have been inserted by malign actors, but likely the result of poor design, manufacturing, and/or testing practices by the DOD suppliers. Again, intent does not matter—the fact that systems supplied by DOD vendors contained multiple cyber vulnerabilities is concerning. Malign actors, given the same opportunities, would undoubtedly exploit the systems to take full advantage of the vulnerabilities to degrade warfighters' capabilities.

Cyber-IT Attack Vector

The fastest growing technologies involve devices contributing to the IoT. These are smart sensor-enabled computing devices that coordinate and communicate over the internet. Common household examples of IoT devices include home assistant speakers, smart thermostats, smart wall plugs, light bulbs, light switches, home energy monitors, house door locks, pet feeders, children's toys, baby monitors, smart electric meters, smart watches and

phones, fitness trackers, smart refrigerators, washers and dryers, microwaves, smart TVs, and the ubiquitous home security camera, to list a few. Statista Research predicted over 75 billion IoT devices will be connected to the internet by 2025.[168]

As noted in the introduction, IoBT devices are increasingly deployed by the DOD as they have robust applications that allow information flow between aircraft, naval vessels, unmanned aerial systems, warfighters, and command posts, creating a unified network that increases situational awareness, risk assessment, and response time.[169] However, there are noted issues with the use of IoT. The Chief Information Officer of the DOD indicated in a 2016 report, *DOD Policy Recommendations for IoT*, that the growing deployment of IoT devices on DOD networks increases the opportunities for cyber compromise by malign actors:[170]

> IoT is already upon us, with millions of these devices already installed in our facilities, vehicles, and medical devices. The newest DoD green buildings have tens of thousands of sensors. The growth of internet-connected medical devices has been similarly exploding. IoT devices have the potential to be incorporated in our weapons and intelligence systems (both intentionally and unintentionally). … However, the immense promise of this technology comes with immense risks. While there have always been risks to DoD sensors and controls, their proprietary nature and isolation limited the possibility of attack. Now, with such capabilities being given Internet access, DoD is entering a quickly deepening pool of vulnerability. At risk are all the things that embrace the Internet of Things (IoT): DoD facilities, equipment, employees, and their possessions—any of which could be used to cause harm.[171]

The report noted that IoT devices expand the DOD's cyber-attack surface through two means relevant to the supply chain. First, many DOD suppliers employ IoT devices during manufacturing and distribution, providing malign actors with opportunities to compromise and disrupt critical manufacturing capabilities. Second, malign actors can compromise the IoT devices themselves during their manufacture and distribution, potentially allowing for the implant of backdoors that could allow unauthorized access to IoT devices deployed on DOD networks. In the latter case, a malign actor need not 'hack' into an IoT device because the device had been outfitted with an

open backdoor during their manufacture. A backdoor allows a malign actor access without authenticating to a system, thereby providing the actor with remote access to not only to the IoT device, but potentially other systems connected to the DOD network.

A reported example of an attack on an IoT device that allowed a malign actor to connect to other computers on a network occurred in a North American casino. In this case, a malign actor penetrated an internet-connected fish tank in the casino.[172] The fish tank contained sensors that were coupled to a computer that measured and regulated food, temperature, and water cleanliness. Once the malign actor connected to the "IoT fish tank," the actor was able to connect to other computers on the casino's network that stored sensitive data, resulting in the exfiltration of 10 GB of data.[173]

The DOD report warned that IoT devices are designed and fielded with minimal security requirements and testing, and the ever-increasing complexity and connectivity of networks could lead to widespread vulnerabilities in civilian and U.S. government infrastructures. This concern has been underscored by leaders in the intelligence community. In his 2016 Worldwide Threat Assessment of the U.S. Intelligence Community, the Director of National Intelligence noted: "In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials."[174]

In 2017, the GAO published a report on a study conducted on the security risks of IoT devices, due to their increasing use by the DOD.[175] Table 1 displays the risks of IoT devices.[176]

According to the GAO report, there are multiple and varied risks involving IoT devices in how they are designed, manufactured, and configured, and unfortunately, there is currently little incentive for some manufacturers to invest in the design and implementation of robust security functions into their products, although new government regulations may change this.[177]

A 2016 DOD report noted that IoT devices will be increasingly used on the battlefield, and if not properly secured, could result in profound negative consequences for missions.[178] The report provided an alarming scenario involving warfighters on the battlefield:

> Imagine that the enemy takes advantage of vulnerabilities in the [IoT] devices or networking, hacking into or compromising these devices and the information they supply. This may allow the enemy

Table 1. Risks of IoT Devices

Device risk	Description of Concern
Supply Chain Threat	The manufacturing origin of IoT devices and related components poses a significant concern. Adversarial countries like China and Russia could embed "exploits," or malicious software, into the hardware of chips and other components used in IoT devices, such as smart meters, to collect and transmit data.
Limited Encryption	Limited encryption in the hardware of IoT devices or the collection and transmission of unencrypted data poses a significant concern. IoT devices have not been designed to facilitate deployment of the latest cryptographic algorithms and protocols, thus posing a range of potential risks, to include eavesdropping, unauthorized access, and device tampering.
Poor Security in Device Design	Current IoT devices have limited security in the design of their hardware and software, including chip design and cybersecurity software. With little built-in security, IoT devices could be compromised without the user's knowledge.
Poor Password Management or Authentication	Poor password management or authentication protocols could lead to DOD industrial control systems or personal IoT accounts being compromised or manipulated by outside hackers.
Patch or Upgrade Deficiencies	As the number of IoT devices increases, the probability of missing—or not implementing—a security upgrade or patch increases, and some devices may not be patchable at all. In addition, a device could be kept in service longer than it is scheduled to receive security or management updates, which at least one DOD component refers to as a "zombie device." Any of these situations could lead to potentially vulnerable or exploitable devices by which malign actors could gain unauthorized access.
Operational Risks	
Rogue Applications	Some device applications—such as gaming applications—could be installed on personal or even DOD smartphones or other devices, which then take pictures or record the user's locations. Such functionality of rogue applications could pose security implications for DOD personnel or facilities.
Adverse Impacts of Devices on Operations Security	IoT devices, including personal smartphones, can tag a person's location—known as geo-tagging—which presents implications for operations security. Officials from three services noted the lack of awareness among their personnel over IoT device capabilities in their environment and the need for behavioral changes.
Rogue Wireless Devices and Insider Threat	An increase in the number of IoT devices could significantly increase DOD's vulnerability to cyber collection. Rogue wireless devices planted by an insider threat or intentionally placed by service personnel (and then compromised) could collect sensitive information or send out data on industrial control systems for purposes of espionage.
Expansion of Attack Surface	The expansion of IoT devices will significantly increase the number of points at which any network can be attacked. IoT devices would provide more attack vectors into a network and a potential platform for massive, distributed attacks.
Unauthorized Communication of Information to Third Parties	Some IoT devices could by design collect and send data back to commercial providers, such as third-party help desks, and DOD components may have little insight into the internet destinations of such data.

> to provide false information to the warfighter and the supporting remote organizations, making decisions and actions they take either unreliable or dangerous. At the same time, they can also see the information that should have gone to the warfighter, giving them the advantage of the situational awareness and further allowing them to take advantage of the confusion they have created through the injection of false information into the warfighter decision making.[179]

The most devastating IoT attack in the civilian domain occurred in October 2016. Dubbed "Mirai," the attack involved a malign actor identifying vulnerable IoT devices on the internet,[180] and then using a list of known default credentials to gain access and infect the devices with malware.[181] Once a device was infected, it transmitted the internet protocol address of the newly infected device to the malign actor. Over 600,000 IoT devices were infected and aggregated into a single interconnected entity called a *botnet*. The malign actor could then send a signal to the botnet to direct massive and overwhelming volumes of internet traffic to websites, rendering them essentially inoperable. Targets included a well-known cybersecurity researcher, as well as the internet traffic company DYN, which provides services for websites like Amazon, Spotify and Twitter.[182] This attack effectively shut down dozens of large websites for several days.

Botnets attack a system's availability, which is the measure of reliable uptime for server or networked computer systems. To maintain battlefield supremacy, IoBT, servers, and networks need close to 100 percent uptime. It is imperative the DOD provides protective and mitigation strategies against attacks to damage availability.

Human Domain Attack Vectors

The average person thinks that cyberattacks require great technical skill and that most attacks are of a technical nature; however, this is not the case. Bruce Schneier, distinguished cybersecurity expert and chief technology officer of Counterpane Internet Security, Inc., once said: "Amateurs hack systems. Professionals hack people." [183] This quote highlights the number of non-technical cyberattacks that are conducted daily against everyone who has a device connected to the internet. Information systems are composed of not only hardware, software, networks, and data, but people as well. As such, malign actors exploit weaknesses in the psychology of human users to influence

them to do something that allows the actor access to information or systems. To do something could mean something as simple as clicking a web link, clicking an email attachment, filling in a web form, or replying to an email. The psychological manipulation of humans is called *social engineering*, which are attempts to trick a user into revealing information that can be used to attack computing systems or networks.[184] The following describes the more common social engineering devices.

As such, malign actors exploit weaknesses in the psychology of human users to influence them to do something that allows the actor access to information or systems.

Human Domain: Phishing

The most common social engineering attack involves *phishing* and its variants. Phishing is an umbrella term for several types of social engineering attacks, and although a social engineering attack can occur through any medium, including text messages, phone calls, regular mail, and even face-to-face, the most common attack vector is through email. Phishing attacks are one of the most common cyberattack vectors across both government and industry.[185] Everyone with an email account has received a phishing email. The goal of the malign actor is to use social engineering to dupe unsuspecting victims to react to the contents of the email. A phishing attack typically involves the actor sending an email under the guise of a seemingly legitimate offer, request, or demand. The malign actor uses a number of psychological principles to influence a user to react to the message, including greed ("Free $50 Amazon gift card!"), fear (a message from the U.S. Internal Revenue Service [IRS] regarding unpaid taxes), empathy (asking for help by a person in distress), and vanity (a message from an attractive person asking to connect). Other psychological forcers are often combined with these methods, such as stressing urgency ("Offer expires at midnight!") and appealing to authority (the IRS example), to create a powerful incentive for the user to respond.

A more formidable variation of phishing is *spear phishing*. Spear phishing involves a message that appears to be from a source the user trusts, such as a family member, friend, chief executive officer (CEO), boss, etc. These attacks are successful because of the element of trust, and sometimes appeal to authority as in the case of a message from a boss or CEO. Spear phishing occurs less frequently than mass email phishing attacks because it requires

additional research on the part of the malign actor. Additionally, *whaling*, a variant of spear phishing, is a term where the target is a high-ranking member of the organization, such as a CEO, board member, or government or military decision maker/leader, etc.

A widely published example of a spear phishing attack involved John Podesta, who at the time was Hillary Clinton's campaign chair during her 2016 Presidential run.[186] Podesta received a spear phishing email pretending to be from Google which indicated that someone from the Ukraine had used his password to login to his Gmail account, and was urged to change his password immediately.[187] The email included an appeal to authority/trust (Google), fear (someone from the Ukraine had his password), and urgency (the message "You should change your password immediately."). After contacting his IT person about the email's legitimacy, Podesta clicked on a "Change Password" button, leading him to website that looked like the Gmail login page, but was in reality a bogus website set up for the purpose of stealing his username and password.[188] Once the malign actor harvested Podesta's credentials, the actor logged into Podesta's Gmail account and downloaded his emails, which were subsequently published on the internet.[189]

Human-Domain: Business Email Compromise (BEC)/Email Account Compromise (EAC)

One of the primary social engineering threats to small- and medium-sized businesses is through BEC or EAC. In BEC attacks, malign actors rely on social engineering techniques to trick unsuspecting employees into authorizing payment of invoices through wire transfer or other means. Email is the primary attack vector.[190] BEC is often facilitated by impersonating the individual responsible for authorizing these wire transfers, such as a CEO or other decision maker. The Federal Bureau of Investigation (FBI) identified five forms of BEC attacks:[191]

1. **Bogus Invoice Scheme.** Malign actors pretend to be suppliers who request wire transfer of funds to an account owned by the actors.
2. **CEO Fraud.** Posing as the company executive, the malign actors send an email to finance department employees, requesting wire transfers to an account owned by the actors.
3. **Account Compromise.** A company executives email account is compromised (e.g., through social engineering) by malign actors, who

then send emails requesting payment of invoices to suppliers listed in the companies email contacts.

4. **Attorney Impersonation.** Malign actors pretend to be lawyers from a firm responsible for sensitive company business.

5. **Data Theft.** Human resources employees are targeted and compromised, typically through social engineering, to obtain personal identifying information regarding key company employees and executives, which can later be used in further targeted attacks.

According to the latest FBI's *Internet Crime Report*, there were 23,775 reports of BEC/EAC attacks in 2019, accounting for $1.7 billion in losses.[192] Even experienced business owners and their employees are subject to these types of attacks. "Shark Tank" judge Barbara Corcoran lost $388,700 in early 2020 through a BEC attack. A malign actor pretending to be Ms. Corcoran's assistant emailed an invoice for a renovation to Ms. Corcoran's bookkeeper.[193] The bookkeeper wired the funds to an account specified in the email. However, the email address did not belong to her assistant, as the malign actor had imitated her assistant's email address by misspelling it by a single letter.[194] The mistake was not identified until the bookkeeper emailed the assistant's correct address for a follow-up. The business owner acknowledged that she would not be able to recover the lost funds.

While the DOD and governmental agencies have multiple checks and balances in acquisition, small suppliers that provide parts and services in the supply chain are less likely to be able to implement stringent safeguards. What if a small- or medium-sized business was attacked, resulting in the loss of the supplier's ability to provide the necessary components to other supply chain participants? Small suppliers arguably are less likely to withstand concerted and persistence cyberattacks, as they may not have the resources or expertise to put into place stringent safeguards.[195] The impetus for a cyberattack may not even be related to the supply chain directly, it may have other motivations—such as theft—which could result in a supplier not being able to deliver. What happens if a critical component cannot be sourced from an alternate supplier? What redundancies would allow a replacement such that the supply chain could continue to function? The FBI warned that a supply chain vendor's current financial state, as well as their capability to meet requirements with current and increased demand, should be considered an

essential part of the supply chain review process.[196] Additionally, a supplier's financial background should be critically reviewed, and consideration should be given to the impact should the provider no longer be capable of fulfilling requirements.[197]

Human Domain: Insider Threats

Insiders are one of the biggest, if not the biggest, threat to cyber systems.[198] An insider is someone authorized to use a system and often has physical access to the system. Examples of insiders include full- or part-time employees, and contractors. A *nearsider* is someone who only has physical access but not granted logical access (i.e., username and password) to a system. For example, a civilian touring a U.S. military installation would be considered a nearsider. The DOD has recognized the potential threats from insiders:[199]

> Some cyber threats also may come from insiders. Malicious insiders may exploit their access at the behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DoD, and national security, can be devastating.[200]

There are several reasons that insiders are insidious threats. Insiders are normally vetted by their employers through background checks, and after vetting, are provided logical access to systems and sometimes physical access.[201] Access provides the insider with increased opportunities for attacking a system. Insiders may also be able to socially engineer an escalation of privileges to higher classified information and systems.[202] Insider threats need not be intentional; threats can also be unintentional or accidental as noted by the GAO: "Insider threats include DOD personnel working directly with adversaries to collect information or DOD personnel unintentionally assisting adversaries through their inattention to cybersecurity (e.g., poor cyber hygiene) or other actions."[203]

An alleged insider attack affecting the supply chain for personal protective equipment (PPE) during the COVID-19 pandemic occurred after a medical device packaging company terminated an employee.[204,205] The employee had administrator access to computer systems containing shipping information, and had added an alternate administrator-level account on the systems

prior to his termination.[206] After the termination, the suspect was alleged to have used the alternate account to remotely connect to the computers that stored shipping information, where he edited roughly 116,000 records and deleted roughly 2,400 records.[207] These alterations disrupted the company's shipping processes, causing delays in the delivery of the equipment to hospitals and other healthcare providers.[208]

Well-known examples of vetted insiders with top security clearances who exfiltrated classified information from U.S. intelligence or law enforcement agencies, or the U.S. military include Edward Snowden[209] (NSA), Joshua A. Schulte[210] (Central Intelligence Agency [CIA]), Robert Hanssen[211] (FBI), Aldrich Ames[212] (CIA), and Chelsea Manning[213] (U.S. Army). Of the five, Snowden, Schulte, and Manning used cyber methods to exfiltrate substantial quantities of classified information.[214]

Takeaways for the SOF Community

As described above, there are multiple methods of cyber compromise in the supply chain, ranging from technically sophisticated attacks requiring great skill and resources, to mundane social engineering attacks easily accomplished through an email. What this suggests is that the SOF community must take a multipronged approach to mitigate supply chain threats. Increased vigilance regarding the provenance of hardware and software, as well as rigorous testing of hardware and software, will be key determinants, among other things, in mitigating any threats posed. Additionally, training, education, and awareness programs regarding social engineering attacks is a crucial factor in reducing the likelihood of these types of attacks occurring. Training, education, and awareness programs should be an ongoing concern, provided annually, and not one-offs. Additionally, alternate sources for products should be identified to ensure that the supply chain remains unbroken should an attack effect a supplier of a crucial component.

Chapter 4. Government Regulations for C-SCRM

Federal agencies have increasingly been tasked with developing and implementing regulations and guidelines to manage supply chain cyber risks.[215] The DOD, in particular, has supported the creation of new policies and management tools to address both the domestic and international risks that exist within the supply chain across a program's life cycle. These efforts are intended to provide the government with an increased ability to examine supplier C-SCRM practices so that greater supplier compliance can be achieved.[216] Managing supply chain risks is vital to ensure that the products and services acquired can be delivered uncompromised to support mission success.

For over 20 years, the U.S. government and other oversight bodies have developed and issued regulations and guidelines for cybersecurity.[217] However, just as there has been a growing and evolving understanding of C-SCRM within academia, there has been an evolution within the government—including the DOD—about how to best mitigate these risks within the supply chain. While the following discussion is not an exhaustive list of applicable policies and regulations, it demonstrates the emerging understanding of the risks the DOD faces within the supply chains.

Prior to the 9-11 attacks, systemic analysis of shipments was not possible, and supply chain risk management fell to risk management and insurance providers.[218] After 9-11, there was a new focus on physical security and more structured methodological approaches, and supply chain risk management shifted to include cyber in 2012.[219] That year, a shift in orientation occurred when President Obama signed the *U.S. National Strategy for Global Supply Chain Security*, which identified the need for greater focus on cyber in supply chains.[220] Additional federal direction was provided in *NIST IR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems* and *NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.[221] *NIST IR 7622* included supply chain visibility and assurance methods, while *NIST 800-161* incorporated the elements of *NIST IR 7622*, but provided greater measures for

ICT by using strategies such as risk identification, risk assessment, and risk mitigation.[222]

In February 2013, the government published *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, which tasked NIST and stakeholders with developing a framework using existing practices, guidelines, and standards, to reduce critical infrastructure risks.[223] The approach in developing the framework emphasized repeatable, flexible, prioritized, and cost-effective approaches to help manage cyber risk.[224]

On 14 March 2014 the DOD released *DOD Instruction* (DODI) *8500.01, Cybersecurity*—a foundational document that provides an updated posture on cybersecurity.[225] This update implemented a common cybersecurity terminology within the federal system, incorporating NIST's *SP 800-53 Security Control Catalog* which focuses on the implementation of early and continual security measures in the acquisition process, and advocates for interoperability, integration, and operational resilience.[226]

Cyber risk management under the DOD is covered by the January 2017 *Risk, Issues and Opportunities Management Guide for Defense Acquisition Programs*,[227] and the RMF is a corresponding but discrete process.[228] In 2014, the DOD adopted the *RMF for DOD IT* when it released *DODI 8510.01*.[229] *RMF for DOD IT* identified that all of DOD's IT falls within the domain of the RMF, and incorporates NIST's RMF framework to align with the recommended processes used by both the intelligence and civilian communities.[230] In addition to covering IT services and IT products, the *RMF for DOD IT* also includes platform IT, information systems, IT R&D, and testing and evaluation for both DOD products as well as contractor products and activities.[231] Key changes from the prior *DOD Information Assurance Certification and Accreditation Process* included replacing information assurance with cybersecurity, replacing the Certification and Accreditation process with the RMF life cycle, updating the security objective to confidentiality, integrity, and availability, and replacing DOD specific terminology with *NIST SP 800-53 Security Control Catalog*, the *Committee on National Security Systems Instruction* (*CNSSI*) *4009, Glossary for Cybersecurity Terms*, and *CNSSI 1253* for categorization purposes.[232]

In 2017, the DOD issued the DFARS Clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Report* for all contracts and requiring compliance by December 31, 2017, unless an acquisition was solely COTS.[233] There are four key elements that contractors must adhere to and

flow down to their subcontractors if a subcontractor's performance requires the use of covered defense information, or the subcontractor provides operationally critical support.[234] These elements include safeguarding covered defense information, reporting cyber incidents, and submitting malicious software and facilitate damage assessment.[235] As part of safeguarding critical information, this regulation also requires contractors and applicable subcontractors to implement *NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.[236]

Emergent Regulations: Cybersecurity Maturity Model Certification (CMMC)

Performance, cost, and schedule alone are insufficient for evaluating suppliers; supplier cybersecurity posture should be included as an equally essential element of the evaluation process. This sentiment was expressed by the joint testimony of the DOD before the House Armed Services Committee (HASC) where C-SCRM in the DOD's supply chain was addressed:[237]

> to elevate the private sector's focus on security, the Department has established a "Deliver Uncompromised" initiative focused on industry delivery of capabilities, services, technologies, and weapons systems that are uncompromised by our malign actors from cradle-to-grave. It aims to establish security as a fourth pillar in acquisition, on par with cost, schedule, and performance, and to create incentives for industry to embrace security, not as a "cost center," but as a key differentiator.[238]

Additionally, the testimony outlined a shift from a compliance-based checklist to a holistic and risk-based approach that is fluid based on current threats and DOD priorities. This pivot also involved creating a plan to protect controlled unclassified information (CUI) that is made available to private industry suppliers. The testimony additionally identified that the integrity of the supply chain needs to be strengthened and that DOD is actively in the process of implementing requirements.

One of these emerging requirements is the *DODI 5000.02, Operation of the Adaptive Acquisition Framework*, dated 23 January 2020, which emphasizes the importance of cybersecurity *throughout* the acquisition process.[239]

DODI 5000.02 tasks program managers with the responsibility of recognizing that a critical part of program planning is cybersecurity. Per the *DODI 5000.02*:

> [cybersecurity] must be addressed early and continuously during the program life cycle to ensure cybersecurity operational and technical risks are identified and reduced and that fielded systems are capable, effective, and resilient.[240]

DODI 5000.02 also provides the transition plan from existing policies to reissued or new policy documents including cybersecurity instructions. The DOD plans to issue a new policy *DODI 5000.CS, Cybersecurity for Acquisition Decision Authorities and Program Managers*, that highlights how cybersecurity should be considered in an acquisition.

There were still gaps in the protection of controlled defense information even after the implementation of both the Framework and *DFARS 252.204-7012*. The Framework was designed to be voluntary and as such had no enforcement capabilities if companies failed to comply. *DFARS 252.204-7012* also presented some challenges, notably, it lacked uniform security, and cybersecurity practices implemented by the defense industrial base (DIB) were inconsistent.[241] Additionally, contractors can demonstrate compliance simply through self-certifications.[242]

Given these concerns, recommendations emerged for the DOD to use third-party assessors to ensure compliance with cybersecurity regulations, rather than self-certifications.[243] The result of this is a new cybersecurity assessment model, the *Cybersecurity Maturity Model Certification* (*CMMC*), published in early 2020, which provides the DOD the capability of certifying companies at different levels of certifications based upon the supplier's cybersecurity posture maturity.[244] The CMMC essentially combines disparate cybersecurity requirements into a single unified standard that can then be applied to the entirety of the DIB supply chain and assessed through third-party assessors.[245]

The CMMC was designed to strengthen the protection of CUI and federal contract information (FCI) within the DIB supply chain.[246] Instead of being a fourth pillar in the acquisition process, along with cost, schedule, and performance, cybersecurity is now considered a foundational requirement.[247] The CMMC effectively shifts from voluntary self-reporting to standards that are measurable and mandatory.[248] The DOD now uses the CMMC levels as

a requirement for contract awards by incorporating the CMMC into the DFARS, issuing an interim rule change to amend *DFARS 252.204.7012* in September 2020.[249] The CMMC will apply to both prime and subcontractors, with prime contractors flowing the relevant requirements down to subcontractors. However, a subcontractor may not be required to have a higher-level certification if they are not working with CUI.[250] Requirements are being phased in so that DIB contractors can adjust over the next five years with full implementation in new DOD contracts occurring by 2026.[251] Current contracts will not be impacted. CMMC Level requirements will be included in request for information (RFI) and request for proposals (RFP) and as a condition of award, the appropriate level must be achieved. Under the CMMC, contractors will no longer be able to self-attest as they did under *DFARS 252.204-7012*; instead, a new independent non-profit CMMC accreditation body will oversee assessment organizations that will employ field licensed assessors.[252] These assessors will then evaluate companies wishing to bid on DOD contracts. Companies must submit to CMMC evaluation every three years. If a company produces only COTS products, CMMC certification will not be required. Figure 3 graphically depicts the five CMMC levels.[253]

The CMMC incorporates several existing frameworks and standards. For

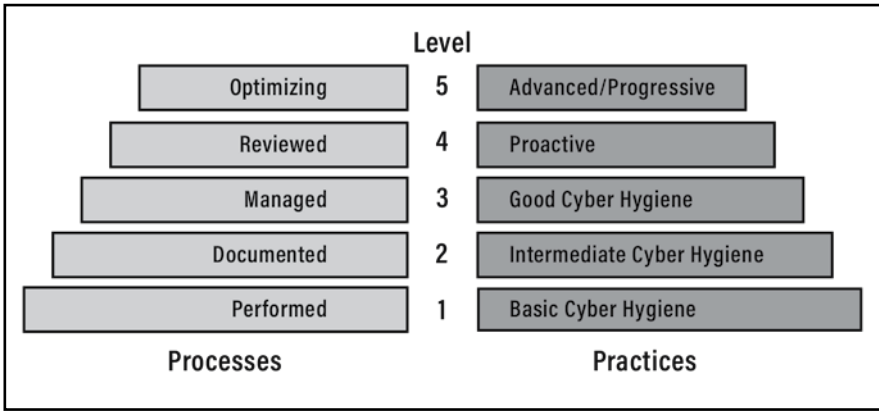

Figure 3. CMMC. Derivative from *CMMC Version 1.02,* created by authors.

example, levels 1-3 correspond to *NISTS 800-171* Rev 1 with additional processes and practices incorporated from other frameworks and standards. The model incorporates five levels of cybersecurity maturity of a company and,

depending on the information to be protected and related threats, provides recommended practices and processes. Practices and processes are organized into domain sets and align to the five levels. Additionally, practices are associated with sets of capabilities within each domain. A company certified to level 1 has processes that are performed and basic cyber hygiene sufficient for the safeguard of FCI, as demonstrated in figure 3. Companies at level 2 have documented processes, they possess intermediate cyber hygiene, and is a maturity transition level progression towards protection of CUI. Level 2 is where the DOD expects mostly small businesses to establish processes and plan for the future. Companies at level 3 have managed processes with good cyber hygiene suitable for the protection of CUI. At level 4, a company's processes are reviewed and have proactive practices. At level 5, a company's processes are said to be optimizing and their practices are advanced/progressive. For both level 4 and 5, the focus is not just to protect CUI but to reduce the risk of advanced persistent threats.[254] It is anticipated that the model will change and evolve as threats change over time.

CMMC covers 17 domains drawn from the *Federal Information Processing Standards Publication 200* security-related areas and also from associated security requirements in *NIST 800-171*, as well as other regulations.[255] The domains include access control, asset management, audit and accountability, awareness and training, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, recovery, risk management, security assessment, situational awareness, systems and communications protections, and system and information integrity.[256] Each domain has associated capabilities, e.g., for access control, capabilities include establishing system access requirements, control of internal system access, control remote system access, and limit data access to authorized users and processes. In total there are 43 capabilities associated with the 17 domains.[257]

Although the CMMC moves acquisition toward more stringent requirements, some have argued that it is not without potential problems. The accreditation body website[258] indicates that there are over 350,000 companies that will have to be assessed, and 10,000 trained assessors will be needed. The companies themselves must bear the cost of assessment, which may be problematic for small- and medium-size non-defense companies who are operating at low margins.[259] Also, there is no clear oversight to determine whether assessments are administered fairly, particularly when it is

the company that is paying the assessors.[260] Finally, there is a possibility of legal disputes when a company is denied a certification; the potential arises for them to bid on a contract which they have worked on for months or even years.[261] It is not clear what happens if a company loses certification in the middle of performance. Does this result in contract termination? Who bears the burden of costs for litigation?

The DOD's position is that the CMMC helps small businesses and that the current self-certification makes competition uneven for small businesses. Under CMMC, the certification level provides a noticeably clear go/no-go decision point; CMMC level 1 has basic cyber hygiene practices which should be low-cost to implement. Another idea to assist small businesses is for primes to allow smaller subcontractors to operate in the prime's secure environment, rather than establishing their own cybersecurity infrastructure.

The DOD's position is that the CMMC helps small businesses and that the current self-certification makes competition uneven for small businesses.

Takeaways for the SOF Community

Government acquisition regulations and guidelines are in a fluid state. Although *DFARS Clause 252.204-7012* and NIST's Framework provide mechanisms for mitigating threats, clearly, they are insufficient, given the changing natures of supply chains and modernization of warfighting technologies. The CMMC, once fully implemented, is expected to provide additional mechanisms for securing the supply chain through third-party vetting of suppliers. However, the CMMC is not a panacea. It is a large-scale change which is likely to have to have tertiary effects on procurers as well as suppliers, as described above. So, while the CMMC may indeed strengthen elements of the supply chain, it may have unintended negative effects on parts of the supply chain that once relied upon—in particular—small- and medium-sized businesses.

Chapter 5. The Hyper-Enabled Operator (HEO) and the Supply Chain

Presented now is a scenario of a hypothetical future HEO who is integrated into an ICT battlefield system that includes personal wearables, weapon systems, vehicles, and other equipment—all of which are equipped with IoBT smart, portable, network-connected sensors allowing for the near real-time collection and processing of data. The warfighter's IoBT includes wearable biometric devices that collect data on the physical and mental state of the warfighter, as well as environmental conditions. These sensors continuously collect context data about the warfighter, equipment, and the environment; the data is aggregated, synthesized, and transmitted upstream to command for feedback and decision-making purposes as demonstrated in figure 4.[262] For simplicity we assume that the IoBT are custom designed and manufactured devices but that also contain some COTS hardware components and software.

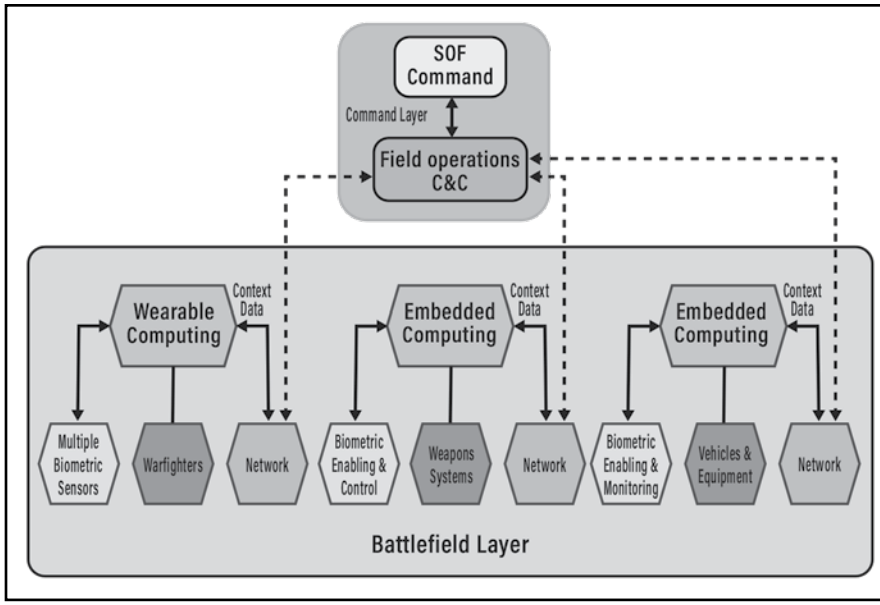

Figure 4. Integrated HEO System. Derivative from *IEEE Cloud Computing* article, created by authors.

As noted earlier, there has been a shift within the DOD to gravitate toward COTS products where feasible and practical. The DOD's acquisition life cycle differs in terminology than that of their suppliers. While the names of the life cycle stages may be different between companies, the stages themselves are similar, are applicable to program-specific products or COTS, and are for both prime and subcontracts. For the scenario, the authors use a unified model of life cycle terminology developed by researchers and graphically depicted earlier in figure 2. The researchers identified the most common terminology used for COTS hardware and software product life cycles through a literature review from government agencies acquisition procedures, industry standards, and academic literature.[263] They used the recurrent terminology to create a single unifying model with common terminology. Differences in terminology emerged between hardware and software, so slightly different product life cycle terminology exists between the two. Seven distinct product life cycle stages were identified:

1. requirements
2. design
3. manufacturing for hardware and development for software
4. testing
5. distribution
6. use and maintenance
7. disposal for both hardware and software[264]

The unified terminology, definitions, and relationship of the life cycle stages are presented in figure 5.[265]

Attack Vectors Across the Product Life Cycle

In this section, for each life cycle stage we identify potential vulnerabilities and cyberattacks, historical examples of vulnerabilities and cyberattacks, and hypothetical attacks against the future warfighter on the battlefield. For hypothetical attacks on the warfighter, we describe unique attacks at each stage so as to not duplicate attacks across multiple stages; in real-world attacks, however, the same attack could be relevant across multiple stages.

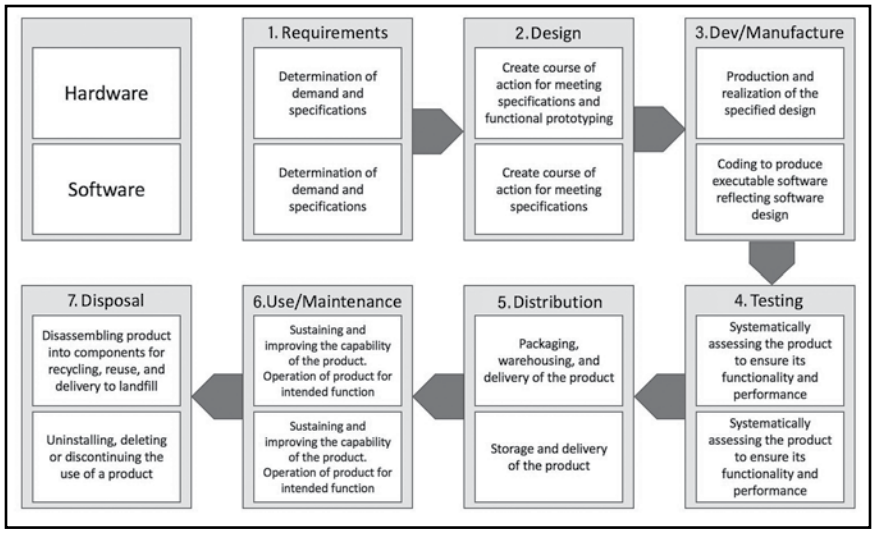

Figure 5. Product Lifecycle Model. Derivative from *Sandia Report* by authors.

The Office of the Under Secretary of Defense for Research and Engineering commissioned research to investigate potential attacks on the supply chain across each of the product life cycle stages.[266] This research culminated in an extensive catalog of attacks for each of the life cycle stages, with the number of potential attacks in a life cycle stage indicating the relative vulnerability or risk of that stage to cyber compromise. The relative frequency of catalogued attacks were then used by others to quantify the relative risk of each life cycle stage to attack using theoretical weights. Figure 6[267] displays theoretical risk weightings—i.e., potentials for attacks—across each stage of the life cycle.[268]

Figure 6 illustrates the comparative theoretical risks to hardware and software across the product life cycle. Adding all weights across the stages adds to 1.0, providing a relative comparison between life cycle stages, and comparisons between software and hardware within a life cycle stage. The lowest weights are .05 for the requirements stage for both hardware and software. The highest weight for software, .25, is the distribution stage; for hardware, .30 is the manufacturing stage. These data points, while theoretical, are representative of the historical cyberattacks described earlier. During the manufacture of hardware—e.g., motherboards, electronic components, etc.—malign actors can substitute counterfeit components, add additional

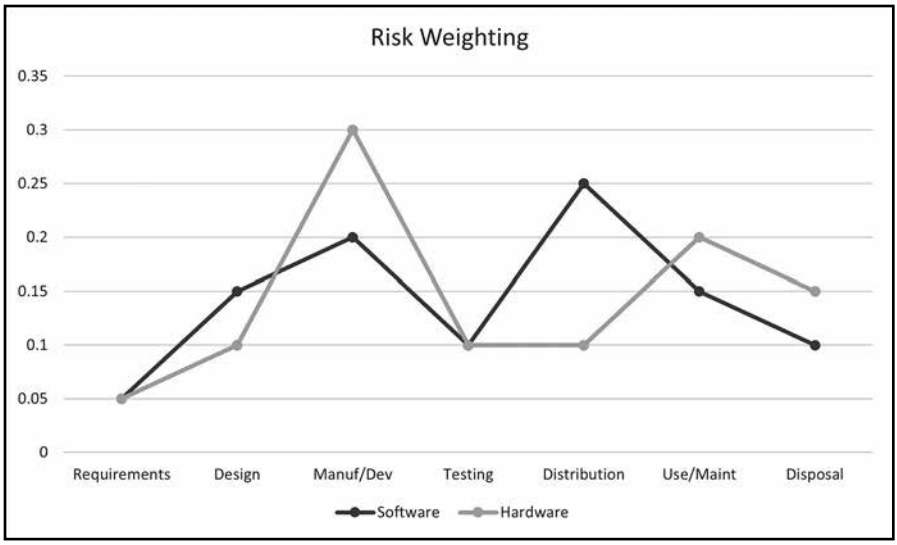

Figure 6. Cyber Supply Chain Risk Weighting (Software vs. Hardware). Graphic created from data in *Sandia Report* by authors.

electronic components that provide remote access, or install malicious firmware.[269] Likewise, the software distribution stage can result in highest level of threat during initial software distribution or during the software update stage through the addition of malicious code. The following are descriptions of each of the aforementioned seven life cycle stages along with their cyber threats and risks; where applicable, actual examples of cyberattacks; and finally, hypothetical cyber threats to the integrated warfighter.

1. **Requirements.** The requirements stage is where the abstract capabilities of the product are identified, based on the needs of the mission. This stage may evolve from a "concept" stage which is a more amorphous description of functionality required for a mission. For program-specific solutions, this is the phase where the government's acquiring agency or department would define requirements based on identified needs. Specific requirements would be identified, and RFPs issued.
   Risks. Risks are considered low in this stage, as requirements may undergo numerous iterative reviews which would likely reveal malicious intent.[270] Data rights assertions can identify the extent to which a program-specific product uses open source software as one way of

assessing risk in the requirements stage. A potential issue may arise once requirements are identified, a supplier for a COTS product has been selected, and systems have been purchased and fielded: the supplier may be acquired by a non-U.S. competitor—or worse, a potential adversary—which may cause mission disruptions. For instance, in 2014 Lenovo Group, a Chinese computer manufacturing company, purchased IBM's low-end server business for $2.3 billion. These servers were installed, and an integral part of, the U.S. Navy's Aegis Combat System.[271] The primary concern for the Navy was that the servers could be potentially compromised during routine maintenance, such as hardware and/or software upgrades, which would be provided by Lenovo.[272] Additionally, there was a concern that information on the weapons system could be accessed remotely by Chinese government agents through a backdoor.[273] Due to these concerns, the Program Executive Office (PEO) for Integrated Warfare Systems' Aegis program office—and the manufacturer of the Aegis Combat System, Lockheed Martin—were required to evaluate alternate hardware solutions to mitigate the impact of the sale.[274] In 2016, the Pentagon's Joint Staff warned the DOD and their personnel against purchasing any computers manufactured by Lenovo.[275] An internal report by the J-2 intelligence directorate stated that cybersecurity officials were concerned that these devices could introduce compromised hardware into the DOD's supply chain—helping China by facilitating cyber intelligence gathering against both classified and unclassified DOD networks.[276]

While the requirements stage is one of the stages least likely to fall under compromise, it is not immune. For instance, during requirements development the descriptions of an IoBT's capabilities may be altered or misrepresented—potentially causing inaccuracies in derived system requirements.[277] Thus, the IoBT may not fully encompass all the functionality as initially conceptualized by the procurer, or functionality may not appear as originally conceptualized. Also, a malign actor may distort software requirements, resulting in errors in the design stage—which again affect the IoBT to fully encompass all functionality as originally conceptualized and required by mission needs.[278] It would be reasonable to conclude that insiders would have the best chance of carrying out these types of attacks.

2. **Design.** The design stage is where activities are engaged to meet the specified requirements, and abstract capabilities from the requirements stage are combined with additional details of the product's components and functionality by designers and engineers.[279] Vulnerabilities may result from intentional acts from malign actors, or non-malicious bad decisions by suppliers. Secure software design is a fundamental part of critical systems where a primary objective is to produce a system that has the necessary authentication, authorization, confidentiality, data integrity, and availability as specified by the product requirements.[280] *Authentication* is defined as a user providing proof of identify to a system, through username and password, personal identification number, or biometric, etc.; *authorization* is defined as the process that ensures that a user has access only to those files and system functions required to perform their job, and no more.[281] Insufficient detail to these requirements can result in some of the issues described previously, such as when DOD system testers identified multiple vulnerabilities in DOD weapons systems, and were able to successfully penetrate the systems.[282]

Risks. Risks in the design stage may just as likely to be caused by unintentional non-malicious acts as intentional acts. Unintentional non-malicious acts may be due to lack of due diligence to speed up production and meet product schedules. From a software perspective, examples include the selection of an inappropriate algorithm; failure to implement error handling in code; or failure to include mechanisms for encryption or digital signing, which can cause the information leakage.[283] On the hardware side, components selected may become obsolete by the time a system is fielded, and OEM components may no longer be available, forcing the DOD to purchase from suppliers where "pedigree is less secure, and provenance is more difficult to track using current procedures."[284] This is a real concern—as approximately 70 percent of electronics in fielded weapons systems are obsolete or no longer in production prior to fielding the systems.[285]

As mentioned above, the design stage can be affected by compromises in the software requirements stage. For instance, a malign actor with access to requirements specifications and/or software design processes and tools can alter them to cause errors in system design.[286]

The result is that the IoBT may not encompass the full functionality as originally conceptualized. Software developers could also fail to implement error handling in the source code, causing IoBT devices to malfunction and provide inaccurate data, or become inoperable. Inaccurate data may be a bigger problem as data are aggregated, synthesized, and directed upstream to command to provide decision makers with an inaccurate picture of the battlefield.

3. **Hardware Manufacturing and Software Development.** Software development is the process of producing source code which is then compiled into executable code that supports the intended functionality identified in the requirements and design stages.[287] Hardware manufacturing involves the concrete production of the specified design through assembled components. In this stage, multiple tiers of the supply chain provide hardware components or subsystems that are then fabricated and assembled into the final product.[288]
Risks. Manufacture of hardware is normally the most complex stage of the hardware life cycle as it involves the most participants and activities.[289] Consequently, there are more potential attack vectors at this stage. Hardware implants—such as extra electronic microchips included on the motherboard that were not part of the original design—can be added, as the Supermicro story described earlier. But this is not a unique case. In 2010, computer manufacturing company Dell acknowledged that some of its PowerEdge servers shipped with malware installed on the motherboard's embedded server management firmware.[290] Unfortunately, there is little detail published on the type of malware or its intended function, but the fact that the malware was found on the server management board (SMB) suggests that the malware might have functioned as a backdoor given the purpose of the SMB is to provide remote access to an authorized administrator. Given that the servers shipped with the malware installed, one might surmise that an insider infected the motherboards, or a third-party supplier was the source. Regardless, this was clearly a supply chain attack.

It is a truism that as system complexity increases, there is an attendant requirement for more lines of source code. Complex systems can contain millions of lines of source code.[291] Estimates vary on the

number of security issues, i.e., "bugs," identified per line of source code, but they range from one bug per 1,000 lines of well-written code up to 25 per 1,000 lines for less well-written code.[292] Using the conservative estimate of one bug per 1,000 of lines of source code, one could extrapolate that a large system with 20,000,000 lines of well-written code could potentially contain 20,000 bugs. Each bug is a potential vulnerability which could affect warfighters' capabilities and mission success. Although most security vulnerabilities in code are not placed maliciously, the potential effects are the same.

In the introduction, there was a description of an early instance of IoBT that involved U.S. Army helmets containing built-in sensors that transmitted sensed data over networks to physicians, who could then assist in diagnosing brain injuries.[293] Future IoBT devices are likely to include biometric sensors to measure the warfighter's physical and mental state, as well as environmental sensors, all of which provide data that are aggregated and synthesized to provide the warfighter and command with an accurate picture of the battlefield.[294] Failure to use encryption, or the use of weak encryption, could allow a malign actor to intercept the data, providing the actor with insight on the warfighter's health, the warfighter's systems in use, troop locations and movements, etc. More problematic, the sensed data could be intercepted, modified, and then transmitted upstream to the command level, providing a false picture of the battlefield. On the hardware side, a malign actor could substitute a modified microelectronics component containing malicious logic, causing false data to be transmitted upstream, providing an unrealistic picture of battlefield and warfighter conditions. The malign actor could also substitute counterfeit components that are less reliable than OEM components, causing the units to fail more quickly.

4. **Testing.** Testing is the systematic assessment of the hardware and software separately, or the system as defined by the integrated hardware and software package. Testing can be a complex activity depending upon the level of testing required. Minimally, a system needs to be tested to ensure that it performs the functions specified in the requirements stage and within designated performance minimums.
Risks. Testing is straightforward: run a series of tests to determine if the system correctly performs the functions as specified in the

requirements and design stages. As mentioned earlier, what is not apparent is the answer to the question "what else can the system do?" Malign actors can add malicious functionality to the source code, which may be triggered by an event or condition. Alternatively, open source code—e.g., common software libraries—may contain latent vulnerabilities or malicious functionality.[295,296] Unless the source code is available for review, it is difficult to identify all functionality if only the compiled executable code is available.

Latent vulnerabilities often elude testing because most testing involves ensuring that the system functions as specified, but may fail to invoke circumstances which might render the system inoperable. For instance, previously discussed was the story of a weapons system that shutdown when DOD security testers performed a simple network scan of the system.[297] A network scan is one of the first activities that malign actors perform when seeking to gain access and control a networked system. A network scan provides the actor with information on what computers are connected and running on the network, as well as what types of network traffic each computer is responding to (e.g., web network traffic, email network traffic, etc.). Accordingly, testing should include functionality testing as well as other forms of testing for activities that a potential malign actor may perform.

Systems often rely on input from humans—such as typing in a text box, typing a keyboard combination, or reading data from other systems. Software accepting data input from any source needs to be tested for out-of-bounds conditions, such as data that is too little, too much, or not in an acceptable format. If a system receives data in a format not expected, it can cause the software to fail, or to behave in an unexpected manner.[298] Securely designed software is expected to identify these conditions and handle them appropriately; if it doesn't, the system may not function as expected or become inoperable.

On the hardware side, counterfeit hardware parts may be identified during quality assurance testing.[299] Testing for malicious hardware modification may require disassembling the system into its component pieces, which is problematic on large scales.[300] As discussed in the introduction, the DOD noted that 15 percent of its parts were identified as counterfeit in the last decade.[301]

Here is the scenario: an HEO has a weapon system outfitted with an IoBT GPS sensor. The system passed testing in the U.S.; however, a malign actor was able to insert malicious functionality—such as a logic bomb—into the code during the software development stage, or during the software update stage. The logic bomb's code is set to execute whenever the latitude and longitude indicate that the IoBT is in enemy territory, causing the weapons system to provide false data, or become inoperable.

5. **Distribution.** Distribution involves the packaging, warehousing, and delivery of a product—system, component, or software—from supplier to end-user customers.[302] For the hypothetical HEO scenario, it is assumed that all hardware comes assembled and software installed where appropriate. Distribution occurs through vetted freight forwarders and normal DOD distribution channels.
Risks. Potential risks occur during product initial shipping, as well as shipping of replacement parts. Freight forwarders are normally vetted by the government and are on an "approved" list; however, each additional layer in the shipping and storage process opens opportunities for malign actors to intercept and modify the systems. As with testing, shipping may also occur within other stages of the life cycle whenever the final product or its components are in transit. For instance, shipping is also required during the maintenance and disposal stages, with multiple participants supporting the transportation of the soon-to-be retired system.[303]

Counterfeit parts or entire systems are another issue in the distribution stage. In 2008, Cisco—the largest manufacturer of network routers[304]—admitted that its partners sold counterfeit Cisco products to the U.S. military.[305] In a leaked FBI PowerPoint presentation that detailed "Operation Cisco Router," the FBI identified the counterfeit products came from Shenzhen, province of China, but were unable to determine if the goods were made by state-sponsored malign actors, or for entities that were for-profit. The FBI noted that the counterfeits could open hardware backdoors, allowing an attacker to gain access and control the router.[306] Additionally, counterfeit products are known to have higher failure rates than OEM equipment, with the FBI noting that one of these counterfeit products caught fire in a government

network due a faulty power supply.[307] Additionally, one company was cited for allegedly selling counterfeit products from China to the U.S. Air Force, U.S. Marine Corps, the Federal Aviation Administration (FAA), universities, financial institutions, defense contractors, and the FBI.[308]

The FBI identified the supply chain issue, finding that Cisco did little or no vetting of "Cisco partners"—noting that "silver" and "gold" level partners were selling the products to the government. The FBI also noted that these problems stem from long standing U.S. government practices of buying from the lowest bidder. At the time, a genuine Cisco router cost $1,375, whereas "gray" market routers cost about a sixth of that price—approximately $234.[309] This example underscores the issue previously described, where procurers may have no insight as to who the participants are in the supply chain outside of the nearest participants.

Shipped items are commonly tracked through radio frequency identification (RFID) tags. RFID are electronic tags that are attached to or embedded in objects for identification and tracking purposes.[310] Components embedded with RFID tags can be tracked using RFID readers that are placed along the distribution path. When an RFID tag is read by an RFID reader, information on product identification and location is transmitted over networks back to the organization for tracking purposes. The security of this information—confidentiality, integrity, and availability—is only as good as the security of the networks over which data are traveling. Imagine several thousand IoBT devices shipped to a battle zone. If a malign actor intercepted RFID data traveling over a network, it might allow the actor to determine the product being shipped, their destination, the number of products in the shipment—and therefore, estimates of number of troops and their locations, etc. This would provide the malign actor with insight on sensitive battlefield operational plans and capabilities.

6. **Use and Maintenance.** During this stage, the end user will make use of the system for its intended functionality, and maintain it to ensure it continues to function. Hardware systems often require maintenance, including regular physical maintenance (e.g., cleaning), and replacing

malfunctioning or worn components. Software updates are common to patch security issues or add additional functionality to a system.

Risks. System misconfiguration—or, lack of configuration—may lead to unseen vulnerabilities. For instance, systems are normally shipped with a set of default credentials that allow the initial administrative user to setup the system for deployment in the field. Changing the default credentials should be an immediate task for the administrator, as leaving default credentials can lead to a malign actor's ability to access the system; as discussed previously, DOD testers were able to gain access to weapons systems because default credentials were not changed.[311]

Software Update Attacks. During this stage, users will maintain their systems through security updates, updating the device's operating system, and installing additional software that also requires updates to patch security issues on a regular basis. Most large software manufacturers use digital certificates[312] to digitally sign software, ensuring software is verified to be from the authentic source and that it has not been modified from its original state. The digital signature process can be thought of as a digital means of "notarizing" software, much like a notary public authenticates signatures on legal documents. When a user installs or updates software, this digital signature is checked for authenticity. Normally, if a malign actor replaces or changes the original file, either a warning message will display or the software installation/update will fail to proceed, or both. Unfortunately, digital certificates are not foolproof as a means of authentication. In 2011, a malign actor—allegedly from Iran—was able to gain access to an account from a trusted partner of the certificate authority[313] Comodo. The malign actor issued nine fraudulent digital certificates for several domains, including mail.google.com, www.google.com, login.skype.com, login.live.com, and several others.[314]

All major operating system and application manufacturers provide regular software updates that remedy security or performance issues. Moreover, many manufacturers support automatic updates so that they occur without manual user intervention, and can be scheduled for off-peak hours so that user activity is not disrupted. Malign actors have exploited these two details to create *software update supply chain*

attacks, which increased 78 percent between 2017 and 2018.[315] A software update supply chain attack is defined as:

> Implanting a piece of malware into an otherwise legitimate software package at its usual distribution location; this can occur during production at the software supplier, at a third-party storage location, or through redirection.[316]

Software update attacks are effective because they exploit a trusted channel (the software manufacturer), and automatic updates allow the malware infections to grow quickly without manual intervention by the malign actor.

In 2019, a software update supply chain attack occurred that involved malware on ASUS laptops. Ostensibly, the malign actors leveraged a backdoor attack, modifying the ASUS Live Update Utility that delivers software updates to laptops and desktops.[317] The software utility was digitally signed with a legitimate digital certificate and hosted on an official ASUS server dedicated to providing updates to ASUS computers.[318] It was estimated that one million users downloaded the utility. The fact that malign actors were able to leverage legitimate digital certificates meant to ensure a file's origin and integrity is cause for alarm.

Ransomware. Another threat during this stage is ransomware. Ransomware, as described earlier in this monograph, is malware that encrypts files on a computing device. The encryption is sufficiently strong enough so that files cannot be decrypted without a decryption key. In a civilian scenario, once the ransomware encrypts the files, a message is presented to the user that explains what has occurred with instructions on how to purchase a decryption key using some form of anonymous cryptocurrency so that there can be no attribution back to the identity of the malign actor(s).[319] The ransomware payload—the actual malware that infects the host computer and encrypts files—often arrives in the form of a legitimate appearing attachment to an email (e.g., an invoice). Once the attachment is clicked by the user, the ransomware silently starts the encryption process. The user is normally unaware of the encryption running until it is too late. Phishing emails are the primary attack vector for ransomware in the

civilian domain, although there is the potential for ransomware to be part of a software update.[320]

Most ransomware is written for versions of the Windows operating system—given that Windows holds 89 percent of total desktop/laptop operating system market share—and therefore remains a bigger target.[321] Although strains of ransomware exist for Apple MacOS and Linux operating systems, as of mid-2020 they are relatively rare; motivated, state-funded malign actors can with no doubt create a strain of ransomware that could target a weapon or support systems running a customized embedded Linux or other operating system. Additionally, ransomware exists for the smart phone operating systems including Android (72 percent market share as of 2020)[322] and Apple iOS (27 percent market share as of 2020).[323,324]

During 2018–2019, there were dozens of local governments that were victimized by ransomware, including Atlanta, GA,[325] Lakeland, FL,[326] Fort Lauderdale, FL,[327] several Louisiana parishes,[328] and over 20 local governments in Texas.[329] According to the 2019 FBI Internet Crime Report, there were 2,047 instances of ransomware reported in that year.[330] However, the number of reported cybercrimes may only represent 10 to 12 percent of the actual total number committed in the U.S. each year.[331] Similar to the Maersk incident discussed previously in this monograph, the reason entire cities were affected by ransomware is that they used versions of Microsoft Windows known to have a vulnerability in its file sharing protocol—allowing a single infected computer to automatically infect other systems across the organization's network.

Cybersecurity Issues with Cloud Services. Private and public companies and organizations are increasingly using cloud services. Cloud services are on-demand services provided over the internet from the cloud provider's servers, obviating the need for an organization to acquire and maintain their own servers and resulting in reduced costs of acquisition and maintenance. Some of the more well-known cloud service providers include Amazon Web Services, Microsoft Azure, Google Cloud, Oracle Cloud, and IBM Cloud. Cloud services range from software and storage on demand, all the way to providing a company with an entire IT infrastructure. Larger corporations relying on cloud services include Target, Walmart, Apple, General Electric,

Instagram, and Netflix.[332] One of the largest entities moving toward use of the cloud is the DOD:

> In September 2017, the Deputy Secretary of Defense issued a memorandum calling for the accelerated adoption of a Department of Defense (DoD) enterprise-wide cloud services solution as a fundamental component of ongoing DoD modernization efforts.[333]

In 2018, the DOD published its *DOD Cloud Strategy* report, which recognized the need for updating warfighter support through innovative technology, such as the cloud:

> The Department of Defense (DoD) has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical. Data and our ability to process data at the ready are differentiators to ensure mission success. Cloud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage.[334]

The DOD's growing use of the commercially available cloud services to store and process highly classified data may improve warfighting effectiveness and mission success, but it also provides an enormous and increasing attack surface for malign actors to compromise—either through external attacks or by malicious insiders employed by the cloud providers. Cloud security provider Armor identified 621 million attacks on cloud customers in 2018, including brute force password attacks, attacks against vulnerable software, web application attacks, and IoT attacks.[335]

The futuristic HEO is situated on the battlefield with multiple IoBT devices and sensors feeding critical data to the warfighter, as well as an upstream to command for battlefield assessment. An IoBT device requires an update downloaded from a "secure" cloud server, and the update is applied; however, a malign insider has modified the update stored on the cloud server to include malicious code that encrypts files after a set period of time. Suddenly, IoBT sensors no longer function—as the operating system files have been encrypted—rendering the IoBT device inoperable. If these updates were automatically applied,

that would mean all IoBT devices would be susceptible to the attack as a matter of course.[336] Or, the update contains malicious logic that causes sensors to transmit inaccurate data to the warfighter and to command, providing a false picture of the battlefield. On the hardware side, an IoBT device may malfunction due to faulty components, but the OEM no longer manufacturers them, requiring the DOD to procure from an alternative source which may not be as well vetted as the OEM—increasing the potential for supply chain vulnerabilities.

7. **Disposal.** Disposal involves the decommissioning and removal of a product at the end of its life.[337] Hardware disposal involves disassembly for reuse, recycling, or destruction, and software disposal includes uninstalling, deleting, or otherwise discontinuing the use of the product.[338] Software disposal requires permanently removing all remnants of software and data from storage devices.
Risks. The number one threat in the disposal stage can be caused by the lack of due diligence in not securely deleting sensitive files from a system's storage device, usually a hard drive. The secure deletion process can be a complicated activity for non-technical users. All computing and electronic devices and media should be subjected to secure deletion procedures, including storage devices such as hard drives and external media such as flash drives, CDs, DVDs, etc., upon disposal.[339]

   The average person thinks that the act of deleting a file permanently removes that file; it does not. When a user deletes a file, all operating systems—regardless of the type of storage device—changes a single "flag" residing in the metadata of the file, and that flag informs the operating system that the storage space used by that file can now be reused if and when necessary.[340] The original file will remain intact and is recoverable until overwritten by more data.[341,342] Anyone with a cyber forensics background can easily recover files deleted from a storage device. The most common way to *securely* delete a file is to overwrite that file with more data.[343] Even with secure delete programs, research has shown that the effectiveness can be spotty, leaving traces of the original file.[344] Governmental agencies, including the DOD and intelligence agencies, have their own guidelines for securely deleting

data—some of which include physical destruction of the device which stored highly sensitive information.[345]

At some point in time, the HEO's IoBT devices will become obsolete, permanently malfunction, or become degraded in some other way. Since these devices are likely to still store information, they will need to be disposed of securely. Note that disposal requires transportation to the location at which the systems will be disassembled, and storage devices securely erased. During transportation, systems could be intercepted and data read from the devices. Also, the compiled code could be extracted and reverse engineered to determine how it functions, which could then be used for future attacks by malign actors.

Takeaways for the SOF Community

Much of the literature would suggest that supply chain attacks begin and end at acquisition and procurement. Clearly, this is an understandably myopic view of the possibilities of cyber compromise for a weapons or support system. Just as important are the manufacturing/development, use/maintenance, and disposal stages of the product life cycle. As government regulations seek to improve mitigation strategies for cyber compromise during acquisition and procurement, they force malign actors to identify new attack vectors for the system compromise. Additionally, the expanded use of cloud services will create a concomitant increase of the DOD's attack surface. The SOF community must be vigilant regarding the manufacturing/development, use/maintenance, and disposal stages, ensuring that these stages are also covered by appropriate regulations and guidelines to reduce the likelihood of compromise.

Chapter 6. SOF Acquisition

As the threats and understanding of C-SCRM evolve, so does the DOD response to it. Two themes have emerged from recent updates. First, cybersecurity has been recognized as foundational and should be a consideration across a products' life cycle. Second, while SOF has long recognized the need for rapid acquisitions, the entire DOD is also moving towards more nimble acquisition processes. This section will review what makes SOF acquisition unique, and will discuss some of the evolving and emergent tools and processes that will assist SOF with C-SCRM moving forward.

SOF Acquisition, Technology and Logistics (AT&L)

The SOF community spans the globe, conducting critical missions and—where the need for operational success is paramount—SOF operators use sophisticated and unique solutions.[346] It is also imperative to get that equipment to the operator quickly. James Guerts, a former United States Special Operations Command (USSOCOM) acquisition executive, summarized the SOF needs in January 2016: "Velocity is my combat advantage. Iteration speed is what I'm after, because if I can go five times faster than you, I can fail four times and still beat you to the target. … That's really what we're going after here."[347]

The SOF Acquisition, Technology, and Logistics Center, established in 1991, is responsible for all USSOCOM research, development, acquisition, procurement, and logistics. It works closely with industry, academia, and government to provide rapid and focused acquisition, technology, and logistics support to warfighters.[348] SOF AT&L consists of eight PEOs: Command, Control, Communications, and Computers; Fixed Wing; Maritime; Rotary Wing; SOF Digital Applications; SOF Support Activity; SOF Warrior; Services; and Special Reconnaissance.[349] There are also four Directorates: Comptroller; Logistics; Procurement; and Science & Technology.[350] Underlying the mission is the SOF acquisition process, unique to the USSOCOM, which is more streamlined than other service branches, allowing for quick delivery of modern capabilities.[351] The SOF AT&L accelerates its force and executes its mission by following four key acquisition principles:

1. Delivers capability to the user expeditiously;
2. Exploits proven techniques and methods;
3. Keeps warfighters involved throughout the process; and
4. Takes risk and manages it.[352]

Recent changes announced by the DOD should also provide additional support for the acquisition velocity that is critical to SOF, as noted by the Under Secretary of Defense for Acquisition and Sustainment: "I'm very proud of our Adaptive Acquisition Framework, because I believe it enables DOD to simplify and speed up the acquisition process. The six different acquisition pathways provide flexibility to apply acquisition authorities and various contract types in a creatively compliant manner." Additional acquisition instructions that have also been updated, signed, and issued include *DODI 5010.44, Intellectual Property Acquisition and Licensing Policy*; *DODI 5000.74, Defense Acquisition of Services*; *DODI 500.80, Operation of Middle-tier of Acquisition*; and *DODI 5000.81, Urgent Capability Acquisition and Software Acquisition Interim Policy.* Additionally, the Under Secretary of Defense for Acquisition and Sustainment noted that the DOD was close to finishing *DODI 5000.01, Defense Acquisition Regulation*.[353]

Another mechanism that allows SOF to be responsive in meeting mission needs is through Other Transaction Agreements, sometimes referred to as OTAs.[354] OTAs provide the flexibility to incorporate commercial industry best practices and standards into awards to develop innovative solutions using both traditional and non-traditional defense contractors as OTAs are easily tailorable.[355] There are three types of OTA agreements: research, prototype, and production. OTAs are not Federal Acquisition Regulation-based procurement contracts, nor are they considered grants, cooperative agreements, or cooperative research and development agreements.[356] OTAs historically were seldom used, however in the last few years they have become much more prevalent in DOD acquisitions.[357] The SOFWERX organization, for example, use OTAs as one of their contracting methods.[358]

SOFWERX

Another way to address future warfighter needs with innovative solutions is through the SOFWERX organization. The SOFWERX platform was created

to solve warfighter challenges through a Partnership Intermediary Agreement between USSOCOM and DEFENSEWERX and is a public facing emissary. SOFWERX describes its mission as two-fold: "1) Create and maintain a platform to accelerate delivery of innovative capabilities to USSOCOM and 2) Facilitate capability refinement through exploration, experimentation and assessment of promising technology."[359] SOFWERX brings together different entities including government, labs, industry, and academia. SOFWERX showed how they bring these different entities together to solve future warfighter problems during one recent event—the Innovation Foundry—held on 10–12 March 2020, which was designed to help USSOCOM identify future capabilities areas for Unconventional Warfare for further technical exploration.[360] Within SOFWERX is the Foundry, a workshop for rapid prototyping and provides tools such as 3D printers, welding, and grinders among other manufacturing tools.[361]

SOFWERX also has a responsive acquisition process to rapidly field solutions for warfighters. For example, one event involved Science and Technology Small Business Innovation Research 20.1 Phase I—which solicited grant applications and proposals to address needs related to a platform agnostic data storage infrastructure and Multi-Full Motion Video Fusion 3D capability—among other topics.[362] The event outcomes demonstrate the commitment to speed, as proposals were evaluated within 30 days and the Small Business Innovation Research evaluation team anticipates contract awards within 90 days.[363]

Additional Tools and Processes for Incorporating Cybersecurity in Acquisition

Defense Acquisition University (DAU) created a tool and associated training called the Cybersecurity and Acquisition Lifecycle Integration Tool (CALIT) to help program and acquisition professionals understand cybersecurity across a product's life cycle.[364] CALIT provides a visual way to understand how these processes interact in order develop cyber-resilient weapon systems.[365]

The DOD's Cyber Security and Information Systems Information Analysis Center developed a detailed chart that visually depicts the myriad of government-issued cybersecurity-related policies and regulations.[366] The DOD Cybersecurity Chart identifies the numerous applicable cybersecurity

policies to visually organize and simplify the information. The chart covers different cybersecurity activities or requirements, such as Secure Data in Transit or Strengthen Cyber Readiness, and are organized under five main categories: Organize, Enable, Anticipate, Prepare, and Authorities. The authorities section provides the legal authorities, policies, operational and subordinate documents that apply.[367]

In 2019, the DOD released *DOD Enterprise DevSecOps Initiative*, a new initiative to shift software to faster and more secure development processes.[368] Development, Security, and Operations (DevSecOps) combines industry best practices to create responsive and secure Government software factories. Under DevSecOps, automated standards, tools, and services will permit the rapid development, deployment, and operations of software applications which are interoperable, flexible, and secure.[369] Additionally, DevSecOps uses a cloud environment permitting the DOD to develop and share capabilities seamlessly. This approach allows small businesses to operate within a secure government environment rather than establishing their own cybersecurity infrastructures. This potentially could help alleviate concerns about the CMMC being a barrier to entry for small businesses.

A companion document to DevSecOps is planned for release that will incorporate security language understandable to auditors who are assigned with accrediting software.[370] A key recognition in the new initiative is that the DevSecOps approach will help remedy the issue in legacy software development practices where cybersecurity has not been a primary concern. DevSecOps shifts incorporating cybersecurity throughout the software development process—from separate, discrete functions to a cross-functional model—where these skill sets work in parallel using a continuous monitoring approach.[371] With DevSecOps, cybersecurity is continuously monitored and applied across the software's life cycle.

The DOD released *OSD DevSecOps Best Practice Guide* Version 1.0, dated 15 January 2020, to assist in the transition to DevSecOps.[372] This best practice guide aids the DOD shifting to DevSecOps, focusing not only on the technical aspects of software development, but the necessity of "organizational cultural changes" that must occur for its successful implementation. While it is reasonable to conclude that a culture changes slowly—and that DOD, as a whole, may take time to transition—the changes that are occurring and the tools that are available can help SOF continue to respond to the mission: supporting the warfighters current and future needs with acquisitions that can

be supported at the appropriate velocity with products and solutions that are delivered uncompromised in order to help the SOF achieve mission success.

Takeaways for the SOF Community

The current SOF acquisition process is unique across the military services. Speed and responsiveness to warfighter needs are important goals. SOF AT&L and SOFWERX provide SOF with the ability to rapidly respond to emergent threats and crises. The introduction of DevSecOps is likely to reduce the attack surface for software, as cybersecurity is no longer an afterthought as with legacy software development, but a required component where security is given its due from the beginning of design all the way through the software development life cycle. Additionally, tools such as the DAU's CALIT and the DOD Cybersecurity Chart provide additional assistance to acquisition personnel in assisting in understanding cybersecurity and acquisition regulations.

Conclusions and the Future of SOF Acquisition

As the Maersk incident illustrates, cyberattacks can have tremendous real-world consequences on the supply chain—consequences that could have profound implications for mission success if delivery of needed supplies, equipment, and information is disrupted. SOF rely on increasingly sophisticated hardware and software-driven products, such as the IoBT, which leaves warfighters vulnerable to an increasingly large attack surface. Current and future warfighting technologies will use even more diverse technologies and components—sourced from global tiered supply chains—making it difficult to ascertain the authenticity of parts and the cyber-resiliency of components, parts, and software. As such, the attack surface is only likely to increase in the future.

Shifts to the DOD's acquisition strategies have also made it increasingly difficult to determine cyber risks in products and software. The shift from traditional program-specific products and manufactured systems to a strategy of using more COTS products—alone, or incorporated into other products—leaves SOF with reduced insight and control into the design and development process of lower-tier suppliers. The benefits of the global supply chain—such as interoperability, and rapid innovation—are all benefits that also threaten the cyber-resilience of products. All these factors combine to present SOF with potential supply chain vulnerabilities through either intentional acts by malign actors, or unintentional acts by suppliers with the potential to negatively impact mission outcomes.

The SOF supply chain is under increasing threats of cyber compromise, as modern warfare has moved to blended operations. The potential for military disruptions is high, as malign actors continue to use multiple threat vectors. Attack vectors include the supply chain, cyber-physical systems, cyber IT, and the human domain. Human domain attacks are perniciously malicious; they take advantage of weaknesses in the psychology of humans, which can only be mitigated through training, education, and awareness programs, combined with healthy doses of vigilance and skepticism.

The notion of cyber-resiliency through C-SCRM is evolving to manage cybersecurity risks in the supply chain. While initially focused on IT

cybersecurity, over the last 20 years C-SCRM has evolved into a blended discipline of cybersecurity, SCM, and risk management. Just as the academic literature has evolved in their understanding of C-SCRM, so has the government's—and, more specifically, the DOD's understanding of C-SCRM. Managing the supply chain to ensure products are delivered uncompromised is critical to SOF mission success. As the DOD transitions to *DODI 5000.02, Operation of the Adaptive Acquisition Framework*, greater importance has been placed on cybersecurity being a foundational element throughout the acquisition process, which specifically addresses that program managers need to recognize cybersecurity as a critical part of program planning. *DODI 5000.CS, Cybersecurity for Acquisition Decision Authorities and Program Managers*, a forthcoming policy identified in *DODI 5000.02*, is intended to provide guidance for acquisitions and program managers on managing cybersecurity in acquisitions. The CMMC defines cybersecurity as a foundational element for suppliers, requiring third-party assessors to evaluate suppliers—and it is a way forward for the DOD to manage cyber supply chain risks. The emergent CMMC guidelines will ensure that the DOD has greater assurances that the government's FCI and CUI data will be protected in the supply chain—as CMMC levels will be specified in RFIs and RFPs—with firms needing to be certified at the level specified to be competitive. The requirement for a certain certification level will flow down from primes to subcontractors as well, putting a greater onus on prime and subcontractors to be responsible for their supplier's cybersecurity posture.

Concerns exist about the implementation of the CMMC—and given that it is emerging, some questions are still outstanding. Concerns do exist about the size and number of companies needing auditing and number of assessors needed to conduct the certifications. The expense of accreditation that companies pay for is of concern, especially for small businesses. With the current structure, there is no oversight to determine the fairness of an evaluation. Legal questions still exist, e.g., what happens if a certification is lost by a contractor in the middle of contract performance, or what if the inability to bid on future programs is lost.

SOF AT&L has strategically used legacy acquisition strategies to ensure speed of delivery of products needed to support the warfighter. The DOD transition to the *DODI 5000.02, Adaptive Acquisition Framework* should allow the SOF community new methods to ensure that mission critical products can be acquired and delivered quickly and securely. Further, the

adoption of the CMMC into the acquisition process ensures that cybersecurity is foundational in a product's life cycle. It is reasonable to conclude that while the CMMC was designed to protect FCI and CUI, the more mature and advanced an organization's cybersecurity posture is, the more likely that other cybersecurity threats—not related to FCI and CUI—can be mitigated or prevented. The new emphasis on product life cycle cybersecurity, management of the supply chains, and more responsive acquisitions within DOD itself will strengthen SOF's ability to more quickly deliver uncompromised, mission-critical products needed by SOF warfighters.

All these measures paint the picture that the DOD is moving toward a holistic life cycle approach to managing cyber supply chain risks. The DOD is shifting its posture on cybersecurity from one where cybersecurity is often an afterthought in products to being a foundational element incorporated throughout a products life cycle. The CMMC is intended to ensure that cyber threats and risks in the supply chain are managed and there are adequate controls to protect FCI and CUI. The government is also taking a more secure and agile approach to software products by creating DevSecOps factories for software development—which permits speedier development than legacy methods—but on a more secure foundation. These changes, when used together, demonstrate how all of these policies can work together to manage cyber supply chain risks across a product's life cycle.

Given the recent release of new and emergent regulations, it would appear one recommendation moving forward is training, education, and awareness for *all* those involved in a product's life cycle, not just acquisition or cybersecurity professionals. Training could also be tailored to specific end-user groups. In addition to training, tools that help end-users conceptualize cybersecurity and C-SCRM could be updated to reflect these changes. For example, CALIT, which shows how cybersecurity fits along a product's life cycle, could be updated to reflect the new policies and instructions. Likewise, the DOD *Cybersecurity Chart*—which is a valuable resource to categorize and map the various policies—could be updated and is a valuable tool to demonstrate the "big picture" as to how all regulations fit into the product life cycle. A highly educated workforce can provide knowledgeable professionals for acquisition teams and help ensure that cybersecurity risks in the supply chain can be addressed throughout a product's life cycle.

C-SCRM is still a new and fluid discipline, requiring continued revisions to keep abreast of changing technologies and cybersecurity threats to the

global supply chain. Now that a more collective understanding of C-SCRM is emerging, it will hopefully be easier to measure and test the effectiveness of these new standards. More research will permit the DOD, government, industry partners, and academia to continue to improve the defenses against malign actors wishing to harm the operational readiness and ability to successfully complete the mission for both the SOF warfighter and the DOD as a whole.

Acronyms

AT&L	Acquisition, Technology, and Logistics
BEC	business email compromise
C-SCRM	cyber supply chain risk management
CALIT	Cybersecurity and Acquisition Lifecycle Integration Tool
CEO	chief executive officer
CIA	Central Intelligence Agency
CIO	chief information officer
CMMC	Capability Maturity Model Certification
CNCI	Comprehensive National Cybersecurity Initiative
CNSSI	Committee on National Security Systems Instruction
COTS	commercial off-the-shelf
CPS	cyber-physical system
CPU	Central Processing Unit
CUI	Controlled Unclassified Information
DAU	Defense Acquisition University
DevSecOps	Development, Security, and Operations
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	United States Department of Homeland Security
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIB	Defense Industrial Base
DOD	Department of Defense
DODI	DOD Instruction

EAC email account compromise

FAA Federal Aviation Administration

FBI Federal Bureau of Investigation

FCI Federal Contract Information

FCC Federal Communications Commission

GAO Government Accountability Office

GB gigabyte

HEO hyper-enabled operator

ICT information communications technology

IoBT Internet of Battlefield Things

IoT Internet of Things

IP internet protocol

IRS U.S. Internal Revenue Service

IT information technology

NIST National Institute of Standards and Technology

NSA National Security Agency

OT operational technology

OTA other transaction agreement

OEM original equipment manufacturer

PEO Program Executive Office

PPE personal protective equipment

R&D research and development

RFI request for information

RFID radio frequency identification tags

RFP	Request for Proposal
RMF	Risk Management Framework
SCM	supply chain management
SMB	server management board
SOF	Special Operations Forces
USSOCOM	U.S. Special Operations Command

Endnotes

1. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.
2. Malware is malicious software whose purpose is to cause harm, steal information, take control of, or perform other unwanted actions on a computing device.
3. Greenberg, "The Untold Story."
4. Greenberg, "The Untold Story."
5. Jonathan Saul, "Global Shipping Feels Fallout from Maersk Cyber Attack," *Reuters*, 29 June 2017, accessed 20 May 2020, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19K2LE.
6. Greenberg, "The Untold Story."
7. Greenberg, "The Untold Story."
8. Catalin Cimpanu, "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover from NotPetya Attack," *BleepingComputer*, 25 January 2018, https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/.
9. Cimpanu, "Maersk Reinstalled."
10. Cimpanu, "Maersk Reinstalled."
11. Jon Boyens, Celia Paulsen, Nadya Bartol, Rama Moorthy, and Stephanie Shankles, "Notional Supply Chain Risk Management Practices for Federal Information Systems," *NIST Computer Security Resource Center*, 16 October 2012, http://dx.doi.org/10.6028/NIST.IR.7622.
12. Defense Advisory Board Task Force on Cyber Supply Chain, *Report on the Defense Advisory Board Task Force on Cyber Supply Chain*, February 2017, https://www.hsdl.org/?view&did=799509.
13. Cimpanu, "Maersk Reinstalled."
14. Matthew P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," NIST, 16 April 2018, accessed 18 May 2020, https://doi.org/10.6028/NIST.CSWP.04162018.
15. U.S. Government Accountability Office, *Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale Vulnerabilities*, GAO-19-128 (Washington, D.C., Government Accountability Office, October 2018), https://www.gao.gov/assets/700/694913.pdf.
16. Philip Craiger and Gary Kessler, "Cybersecurity," to appear in *Combating Terrorism in the 21st Century: American Laws, Strategies, and Agencies*, Vol. 2 (Santa Barbara, CA: ABC-CLIO, 2020).
17. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*.

18. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*.
19. "Cyber Supply Chain Risk Management," *NIST*, accessed 3 May 2020, https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management, para 3.
20. Deborah J. Bodeau, Richard D. Graubart, Jeffrey Picciotto, and Rosalie McQuaid, "Cyber Resiliency Engineering Framework," *MITRE Corporation*, 11 May 2016, https://www.mitre.org/publications/technical-papers/cyber-resiliency-engineering-framework.
21. Lori Cameron, "What Is the Internet of Military/Battlefield Things (IoMT/IoBT)?" *IEEE Computer Society*, accessed 4 April 2020, https://www.computer.org/publications/tech-news/research/internet-of-military-battlefield-things-iomt-iobt.
22. Alexander Kott, Ananthram Swami, and Bruce West, "The Internet of Battle Things," *Computer*, no. 49 (2016): 70–75.
23. "SRI International Leading Security Research for U.S. Army Research Lab Initiative to Develop and Secure the Internet of Battlefield Things (IoBT)," *PR Newswire*, 27 June 2018, https://www.prnewswire.com/news-releases/sri-international-leading-security-research-for-us-army-research-lab-initiative-to-develop-and-secure-the-internet-of-battlefield-things-iobt-300601689.html.
24. George Seffers, "Defense Department Awakens to Internet of Things," *SIGNAL Magazine*, 16 January 2015, https://www.afcea.org/content/?q=defense-department-awakens-internet-things.
25. Kott, et. al., "The Internet of Battle."
26. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*.
27. Adapted from: Paul R. Popick and Melinda Reed, "Requirements Challenges in Addressing Malicious Supply Chain Threats," *Insight* 16, no. 2 (2013): 23–27, https://doi.org/10.1002/inst.201316223.
28. U.S. Government General Accountability Office, "Information Security: Supply Chain Risks Affecting Federal Agencies," GAO-18-667T (Washington, D.C., Government Accountability Office, 2018), accessed 12 March 2020, https://www.gao.gov/assets/700/693064.pdf.
29. Marcus Weisgerber and Patrick Tucker, "Pentagon Creates 'Do Not Buy' List of Russian, Chinese Software," *Defense One*, 27 July 2018, https://www.defenseone.com/threats/2018/07/pentagon-creates-do-not-buy-list-russian-chinese-software/150100/.
30. Marcus Weisgerber, "Pentagon Delays Deadline for Military Suppliers to Meet Cybersecurity Rules," *Defense One*, 14 December 2017, https://www.defenseone.com/business/2017/12/pentagon-delays-deadline-military-suppliers-meet-cybersecurity-rules/144549/.
31. Popick and Reed, "Requirements Challenges," 25.
32. Adapted from Sunny L. He, Natalie H. Roe, Evan C.L. Wood, Noel Nachtigal, and Jovana Helms, "Model of the Product Development Lifecycle," *Sandia Report* SAND20159022, 2015, accessed 29 May 2020, https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2015/159022.pdf.

33. Defense Advisory Board Task Force on Cyber Supply Chain, *Report on the Defense Advisory Board Task Force on Cyber Supply Chain*, 2017, https://www.hsdl.org/?view&did=799059.
34. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, 6.
35. "Cyber Supply Chain Risk Management," *NIST Computer Security Resource Center*, accessed 2 April 2020, https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.
36. Paul Wagner, "Combating Counterfeit Components in the DOD Supply Chain," *Defense Systems Information Analysis Center Journal* 2, no. 2 (2015): 9–15.
37. "China Knows All About the F-35 and F-22 (Thanks to the Data It Stole)," *National Interest*, 6 November 2019, https://nationalinterest.org/blog/buzz/china-knows-all-about-f-35-and-f-22-thanks-data-it-stole-61912.
38. Dan Goodin, "'Unauthorized Code' in Juniper Firewalls Decrypts Encrypted VPN Traffic," *Ars Technica*, 17 December 2015, https://arstechnica.com/information-technology/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/.
39. David Volodzko, "The Trade War with China and the Problem with Intellectual Property Rights," *Forbes*, 12 November 2018, https://www.forbes.com/sites/davidvolodzko/2018/11/11/the-trade-war-with-china-and-the-problem-with-intellectual-property-rights/#1512e851728e.
40. Katie Bo Williams, "Cisco Routers Attacked by Hackers In Four Countries," *The Hill*, 15 September 2015, https://thehill.com/policy/cybersecurity/253646-cisco-routers-seized-by-hackers-in-four-countries.
41. Kurt Marko, "How a Scanner Infected Corporate Systems and Stole Data: Beware Trojan Peripherals," *Forbes*, 15 July 2014, https://www.forbes.com/sites/kurtmarko/2014/07/10/trojan-hardware-spreads-apts/#6392f6132536.
42. Peter Robison, "Boeing's 737 Max Software Outsourced to $9-an-Hour Engineers," *Bloomberg*, 28 June 2019, https://www.bloomberg.com/news/articles/2019-06-28/boeing-s-737-max-software-outsourced-to-9-an-hour-engineers.
43. Brian Toohey, "Counterfeit Semiconductors—A Clear and Present Threat," Testimony Before Senate Committee on Armed Services, 8 November 2011, https://www.armed-services.senate.gov/imo/media/doc/Toohey%2011-08-11.pdf.
44. U.S. Congress, Senate, Committee on Armed Services, *Inquiry into counterfeit electronic parts in the Department of Defense supply chain: report of the Committee on Armed Services*, 112th Congress, 2d sess., 2012, S. Rep. 112-167, accessed 4 May 2020, https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf.
45. Boyens, et al., "Notional Supply Chain Risk Management Practices for Federal Information Systems."
46. Ray Dunham, "The DFARS Compliance & NIST 800-171 Implementation Requirements," *Linford & Company LLP*, 9 August 2017, https://linfordco.com/blog/dfars-compliance-nist-800-171/.

47. Ronald Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, and Mark Riddle, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," *NIST*, 16 December 2016, https://doi.org/10.6028/NIST.SP.800-171r1.

48. Weisgerber, "Pentagon Delays."

49. National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity v11," 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

50. Department of Defense, "Press Briefing by Under Secretary of Defense for Acquisition & Sustainment," 31 January 2020, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/.

51. Ivan Boatner, Alisa Chestler, and Joshua Mullen, "New DOD Cybersecurity Certification Holds Key to Contracts," *Bloomberg BNA News*, 23 March 2020, https://news.bloomberglaw.com/tech-and-telecom-law/insight-new-dod-cybersecurity-certification-holds-key-to-contracts.

52. Nicole Perlroth, "Boeing Possibly Hit by 'WannaCry' Malware Attack," *New York Times*, 29 March 2018, accessed 29 May 2020, https://www.nytimes.com/2018/03/28/technology/boeing-wannacry-malware.html.

53. Defense Science Board, *DSB Task Force on Cyber Supply Chain*, 1.

54. For instance, from 1999 to 2015 the Basic Input Output System (BIOS), firmware used in personal computers, increased in complexity by a factor of 10^6.

55. Christopher A. Nissen, John E. Gronager, Robert S. Metzger, and Harvey Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to Changing Character of War," MITRE Corporation, August 2018, https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security, 9.

56. Nissen, et al., "Deliver Uncompromised," 9.

57. U.S. Government General Accountability Office, *Weapons Systems Cybersecurity*.

58. John T. Mentzer, William DeWitt, James S. Keebler, Soonhong Min, Nancy W. Nix, Carlo D. Smith, and Zach G. Zacharia, "Defining Supply Chain Management," *Journal of Business Logistics* 22, no. 2 (2001): 1–25.

59. Mentzer, et al., "Defining Supply Chain Management," 4

60. Mentzer, et al., "Defining Supply Chain Management,"18.

61. Christine Harland, Eugene Schneller, and Guido Nassimbeni, *The SAGE Handbook of Strategic Supply Management* (London: SAGE Publications, 2013).

62. Evelyne Vanpoucke, Ann Vereecke, and Steve Muylle, "Leveraging the Impact of Supply Chain Integration through Information Technology," *International Journal of Operations & Production Management* 37, no. 4 (2017): 510–30, https://doi.org/10.1108/ijopm-07-2015-0441.

63. Andrii Boiko,Vira Shendryk, and Olha Boiko, "Information Systems for Supply Chain Management: Uncertainties, Risks and Cyber Security," *Procedia Computer Science* 149 (2019): 65–70, https://doi.org/10.1016/j.procs.2019.01.108.
64. Harland, et al., *The SAGE Handbook*.
65. Harland, et al., *The SAGE Handbook*.
66. U.S. Government General Accountability Office, *Weapons Systems Cybersecurity*, 2–3.
67. Elizabeth A. McDaniel, "Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness," *Issues in Informing Science and Information Technology*, no. 10 (2013): 313–24, accessed 29 May 2020, https://doi.org/10.28945/1813.
68. National Institute of Standards and Technology, "Cyber Supply Chain Risk Management," accessed 20 March 2020, https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management.
69. National Institute of Standards and Technology, "Cyber Supply Chain."
70. John Rollings and Anna C. Henning, "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations," U.S. Library of Congress, Congressional Research Service, 10 March 2009, https://fas.org/sgp/crs/natsec/R40427.pdf.
71. Rollings and Henning, "Comprehensive National Cybersecurity."
72. McDaniel, "Securing the Information," 313–24.
73. McDaniel, "Securing the Information," 313–24.
74. McDaniel, "Securing the Information," 313–24.
75. McDaniel, "Securing the Information," 313–24.
76. Richard J. Harknett and James A. Stever, "The New Policy World of Cybersecurity," *Public Administration Review* 71, no. 3 (2011): 455–60, https://www.researchgate.net/publication/230148385_The_New_Policy_World_of_Cybersecurity.
77. Jill R. Aitoro, "The comprehensive national cybersecurity initiative," *Nextgov*, 1 June 2009, https://www.nextgov.com/cybersecurity/2009/06/the-comprehensive-national-cybersecurity-initiative/43940/.
78. Harknett and Stever, "The New Policy," 455–60.
79. Aitoro, "The comprehensive."
80. Aitoro, "The comprehensive."
81. Aitoro, "The comprehensive."
82. Aitoro, "The comprehensive."
83. William Jackson, "White House Lifts the Veil on Bush Cybersecurity Initiative," *GCN*, 2 March 2010, https://gcn.com/articles/2010/03/02/rsa-cnci-declassified.aspx.
84. Obama White House Archives, "The Comprehensive National Cybersecurity Initiative," accessed 27 May 2020, https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative.

85. Obama White House Archives, "The Comprehensive."
86. Obama White House Archives, "The Comprehensive."
87. Obama White House Archives, "The Comprehensive."
88. Obama White House Archives, "The Comprehensive."
89. Harknett and Stever, "The New Policy," 455.
90. Scott Borg, "Securing the Supply Chain for Electronic Equipment," Obama White House Archives, accessed 20 April 2020, https://obamawhitehouse.archives.gov/files/documents/cyber/ISA - Securing the Supply Chain for Electronic Equipment.pdf.
91. Borg, "Securing the Supply."
92. This is often referred to as business continuity planning.
93. Borg, "Securing the Supply."
94. Borg, "Securing the Supply."
95. Borg, "Securing the Supply."
96. Valentin-Petru Mazareanu, "Considerations on Risk in Supply Chain Management Information Systems Implementation," *Amfiteatru Economic* 15, no.33 (2013): 128–39, https://www.researchgate.net/publication/298453782_Considerations_on_Risk_in_Supply_Chain_Management_Information_Systems_Implementation.
97. Mazareanu, "Considerations on Risk," 128–39.
98. McDaniel, "Securing the Information," 313–24.
99. McDaniel, "Securing the Information," 313–24.
100. McDaniel, "Securing the Information," 313–24.
101. Sandor Boyson, "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems," *Technovation* 34, no. 7 (2014): 342–53, https://www.sciencedirect.com/science/article/pii/S0166497214000194.
102. Boyson, "Cyber Supply Chain," 342–53.
103. Boyson, "Cyber Supply Chain," 342–53.
104. Boyson, "Cyber Supply Chain," 342–53.
105. Boyson, "Cyber Supply Chain," 342–53.
106. Boyson, "Cyber Supply Chain," 342–53.
107. Boyson, "Cyber Supply Chain," 342–53.
108. Boyson, "Cyber Supply Chain," 342–53.
109. Boyson, "Cyber Supply Chain," 342–53.
110. Boyson, "Cyber Supply Chain," 342–53.
111. Boyson, "Cyber Supply Chain," 342–53.
112. Boyson, "Cyber Supply Chain," 342–53.
113. Boyson, "Cyber Supply Chain," 342–53.

114. Boyson, "Cyber Supply Chain," 342–53.
115. Boyson, "Cyber Supply Chain," 342–53.
116. Luca Urciuoli, "Cyber-Resilience: A Strategic Approach for Supply Chain Management," *Technology Innovation Management Review* 5, no. 4 (2015): 13–8, https://doi.org/10.22215/timreview/886.
117. Urciuoli, "Cyber-Resilience," 13–18.
118. Urciuoli, "Cyber-Resilience," 13–18.
119. Urciuoli, "Cyber-Resilience," 13–18.
120. Urciuoli, "Cyber-Resilience," 13–18.
121. Marjorie Windelberg, "Objectives for Managing Cyber Supply Chain Risk," *International Journal of Critical Infrastructure Protection* 12 (2016): 4–11, https://doi.org/10.1016/j.ijcip.2015.11.003.
122. Windelberg, "Objectives for Managing," 4–11.
123. Windelberg, "Objectives for Managing," 4–11.
124. Windelberg, "Objectives for Managing," 4–11.
125. Om Pal, Vandana Srivastava, and Bashir Alam, "Cyber Security Risks and Challenges in Supply Chain," *International Journal of Advanced Research in Computer Science* 8, no. 5 (2017), 662–66, https://doi:10.26483/ijarcs.v8i5.3385.
126. Pal, et al., "Cyber Security Risks," 662–66.
127. Pal, et al., "Cyber Security Risks," 662–66.
128. Pal, et al., "Cyber Security Risks," 662–66.
129. Pal, et al., "Cyber Security Risks," 662–66.
130. Pal, et al., "Cyber Security Risks," 662–66.
131. Pal, et al., "Cyber Security Risks," 662–66.
132. Pal, et al., "Cyber Security Risks," 662–66.
133. Brett Massimino, John V. Gray, and Yingchao Lan, "On the Inattention to Digital Confidentiality in Operations and Supply Chain Research," *Production and Operations Management* 27, no. 8 (2018): 1492–1515, https://doi.org/10.1111/poms.12879.
134. Massimino, et al., "On the Inattention," 1492–1515.
135. Massimino, et al., "On the Inattention," 1492–1515.
136. Massimino, et al., "On the Inattention," 1492–1515.
137. William Ho, Tian Zheng, Hakan Yildiz, and Srinivas Talluri, "Supply Chain Risk Management: a Literature Review," *International Journal of Production Research* 53, no. 16 (2015): 5031–69, https://doi.org/10.1080/00207543.2015.1030467.
138. Ho, et al., "Supply Chain Risk," 5031–69.
139. Ho, et al., "Supply Chain Risk," 5031–69.
140. Ho, et al., "Supply Chain Risk," 5031–69.

141. U.S. Government Accountability Office, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C., Government Accountability Office, 2018), accessed 29 May 2020, https://www.gao.gov/assets/700/693064.pdf.
142. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* v11, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
143. U.S. Government Accountability Office, *Information Security*, 9.
144. U.S. Government Accountability Office, *Information Security*, 9.
145. Compiled software is the executable code that runs and is the product of human-readable "source code" that are the programmatic computer instructions.
146. Sharon Gaudin, "Ex-UBS Systems Admin Sentenced to 97 Months in Jail," *Information Week*, 13 December 2006, https://www.informationweek.com/ex-ubs-systems-admin-sentenced-to-97-months-in-jail/d/d-id/1049873.
147. Gaudin, "Ex-UBS Systems."
148. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, 6.
149. A CPU is a core component of all computing devices that executes instructions and is considered the "brains" of the computer.
150. Catalin Cimpanu, "AMD Processors from 2011 to 2019 Vulnerable to Two New Attacks," *ZDNet*, 7 March 2020, https://www.zdnet.com/article/amd-processors-from-2011-to-2019-vulnerable-to-two-new-attacks/.
151. Samuel Gibbs, "Spectre and Meltdown Processor Security Flaws—Explained," *The Guardian*, 4 January 2018, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-computer-processor-intel-security-flaws-explainer.
152. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*.
153. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, ii.
154. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, ii.
155. A backdoor is a covert channel for bypassing normal authentication and encryption often used by malign actors.
156. The following story has been denied by several of the primary participants. *Bloomberg Business*, the publisher of the article and its investigators, wrote that the report was the result of over a yearlong investigation involving 100 interviews with seventeen sources that included government officials and insiders at the companies. *Bloomberg Business* stands by this story to date. Nevertheless, it is an important story considering the players as well as the potential targets of the hardware implants.
157. A motherboard is the main printed circuit board in a personal computer, usually consisting of a central processing unit, main system memory, and additional components necessary to the device's operation.
158. Jordan Robertson and Jacob Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies." *Bloomberg*, 4 October 2018, https://www.

bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

159. Dan Goodin, "If Supermicro Boards Were so Bug-Ridden, Why Would Hackers Ever Need Implants?" *Ars Technica*, 11 October 2018, https://arstechnica.com/information-technology/2018/10/supermicro-boards-were-so-bug-ridden-why-would-hackers-ever-need-implants/.
160. Firmware is software or a set of instructions that are programmed into a hardware device. Firmware provides the necessary instructions as to how computer hardware devices communicate with the other computer hardware.
161. Sean Lyngaas, "DHS, Apple Continue to Push Back on Bloomberg Supply Chain Story," *CyberScoop*, 8 October 2018, https://www.cyberscoop.com/dhs-bloomberg-supply-chain-story-apple-amazon-denial/.
162. Edward R. Griffor, Christopher Greer, David A. Wollman, and Martin J. Burns, "Framework for Cyber-Physical Systems: Volume 1, Overview," *NIST*, 10 November 2018, https://www.nist.gov/publications/framework-cyber-physical-systems-volume-1-overview.
163. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*, 11.
164. The specific weapons systems tested were not identified in the report.
165. Penetration testing is an *authorized* "virtual" cyberattack by an approved party on a computer system and/or network that is performed to assess the security of the systems.
166. Escalating privileges are when a user with restricted capabilities on a system can increase their capabilities above which they are authorized to do so.
167. Scanning is a simple and common cyber reconnaissance activity used in a precursor to an attack, requires no technical expertise, and uses widely available open source software.
168. Statista Research Department, "IoT: Number of Connected Devices Worldwide 2012–2025," *Statista*, 19 February 2020, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.
169. Cameron, "What Is the Internet."
170. Department of Defense, *DOD CIO: Policy Recommendations for the Internet of Things (IoT)*, December 2016, https://www.hsdl.org/?view&did=799676.
171. Department of Defense, *DOD CIO*, 1.
172. Alex Schiffer, "How a Fish Tank Helped Hack a Casino," *Washington Post*, 21 July 2017, https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/.
173. Schiffer, "How a Fish."
174. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," U.S. House of Representatives. House Permanent Select Committee on Intelligence, 9 February 2016, https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf

175. U.S. Government Accountability Office, *Internet of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD*, GAO-17-688 (Washington, D.C., Government Accountability Office, 2017), accessed 29 March 2020, https://www.gao.gov/assets/690/686203.pdf.
176. U.S. Government Accountability Office, *Internet of Things*, 11.
177. Anecdotally, one of the authors of this monograph, with 20 years of cybersecurity experience, conducted an *ad hoc* review of IoT security cameras sold on Amazon.com. The author identified several inexpensive China-manufactured security cameras for as little as $10 per camera. Alternatively, security cameras with more robust cybersecurity cost $129 or more per camera. The difference in price was clearly reflected, in part, by the need to design, test, and implement security mechanisms for the more expensive device.
178. Department of Defense, *DOD CIO*.
179. Department of Defense, *DOD CIO*, C4.
180. This entire process can be automated easily, and there is even a website, http://shodan.io, that automatically scans for IoT devices connected to the internet and allows users to search for them.
181. Ben Herzberg, Igal Zeifman, and Dima Bekerman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis," *Imperva*, 26 October 2016, https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/.
182. Josh Fruhlinger, "The Mirai Botnet Explained: How IoT Devices Almost Brought Down the Internet," *CSO Online*, 9 March 2018, https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.
183. Bruce Schneier, "Schneier on Security," *Schneier on Security, Crypto-Gram*, 1 March 2013, https://www.schneier.com/blog/archives/2013/03/phishing_has_go.html.
184. Paul Cichonski, Tom Millar, Tim Grance, and Karen Scarfone, "Computer Security Incident Handling Guide," *NIST*, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2.
185. Executive Office of the President of the United States, "Federal Cybersecurity Risk Determination Report and Action Plan," May 2018, https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf.
186. Kevin Murnane, "How John Podesta's Emails Were Hacked and How To Prevent It From Happening To You," *Forbes*, 21 October 2016, https://www.forbes.com/sites/kevinmurnane/2016/10/21/how-john-podestas-emails-were-hacked-and-how-to-prevent-it-from-happening-to-you/.
187. Joe Uchill, "Typo Led to Podesta Email Hack: Report," *The Hill*, 13 December 2016, https://thehill.com/policy/cybersecurity/310234-typo-may-have-caused-podesta-email-hack.
188. Uchill, "Typo Led to Podesta."

189. Raphael Satter, "Inside story: How Russians hacked the Democrats' emails," *Associated Press News*, 4 November 2017, accessed 29 May 2020, https://apnews.com/dea73efc01594839957c3c9a6c962b8a/Inside-story:-How-Russians-hacked-the-Democrats'-emails.
190. Mark Guntrip, "FBI Reports $12.5 Billion in Global Financial Losses Due to Business Email Compromise and Email Account Compromise," *Proofpoint*, 27 January 2019, https://www.proofpoint.com/us/corporate-blog/post/fbi-reports-125-billion-global-financial-losses-due-business-email-compromise.
191. Federal Bureau of Investigation, "2018 Internet Crime Report," 22 February 2019, https://pdf.ic3.gov/2018_IC3Report.pdf.
192. Federal Bureau of Investigation, "2019 Internet Crime Report," 11 February 2020, https://pdf.ic3.gov/2019_IC3Report.pdf.
193. Jordan Valinsky, "Shark Tank Host Loses $400,000 in a Scam," *CNN*, 27 February 2020, https://www.cnn.com/2020/02/27/business/barbara-corcoran-email-hack-trnd/index.html.
194. There is a similar form of deception malign actors use, called "typo squatting," to trick people to visit an alternate website rather than an authenticate website, for example: "Am0zon.com," instead of "Amazon.com."
195. Boatner, et al., "New DOD."
196. Federal Bureau of Investigation, "Best Practices in Supply Chain Risk Management for the U.S. Government," accessed 23 March 2020, https://www.fbi.gov/file-repository/scrmbestpractices-1.pdf.
197. Federal Bureau of Investigation, "Best Practices."
198. Nissen, et al., "Deliver Uncompromised."
199. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DoD-Strategy-for-Operating-in-Cyberspace.pdf.
200. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, 3.
201. There is an old hacker adage that says: "If I have physical access to the system, then I own the system."
202. That is, the insider could use social engineering principles to trick someone to provide them with information that would allow them more access to information than required (thus the term escalation of privileges).
203. U.S. Government Accountability Office, *Internet of Things*, 12.
204. U.S. Department of Justice, "Former Employee of Medical Packaging Company Charged with Sabotaging Electronic Shipping Records Leading to the Delay of PPE to Healthcare Providers," 16 April 2020, https://www.justice.gov/usao-ndga/pr/former-employee-medical-packaging-company-allegedly-sabotages-electronic-shipping.

205. The employee was indicted by the U.S. Department of Justice, but not yet convicted as of June 2020.
206. It is common to remove a terminated employee's access to computer systems. However, the addition of an additional account which could be used as a backdoor could be easily overlooked.
207. U.S. Department of Justice, "Former Employee."
208. U.S. Department of Justice, "Former Employee."
209. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (New York: Metropolitan Books/Henry Holt, 2014).
210. Adam Goldman, "New Charges in Huge C.I.A. Breach Known as Vault 7," *New York Times*, 19 June 2018, https://www.nytimes.com/2018/06/18/us/politics/charges-cia-breach-vault-7.html.
211. Federal Bureau of Investigation, "Robert Hanssen," 18 May 2016, https://www.fbi.gov/history/famous-cases/robert-hanssen.
212. Federal Bureau of Investigation, "Aldrich Ames," 18 May 2016, https://www.fbi.gov/history/famous-cases/aldrich-ames.
213. Matthew Shaer, "The Long, Lonely Road of Chelsea Manning," *New York Times*, 12 June 2017, https://www.nytimes.com/2017/06/12/magazine/the-long-lonely-road-of-chelsea-manning.html.
214. The Snowden, Schulte, and Manning events occurred recently when computer technology is ubiquitous, and all are considered to be fairly expert with computers, thus the difference.
215. Chris Jaikaran, "Cyber Supply Chain Risk Management: An Introduction," *U.S. Library of Congress*, Congressional Research Service, 20 June 2018, https://fas.org/sgp/crs/homesec/IF10920.pdf.
216. "Six Recent Government Supply Chain Risk and Cybersecurity Initiatives," *Akin Gump*, 13 August 2018, https://www.akingump.com/en/news-insights/six-recent-government-supply-chain-risk-and-cybersecurity.html.
217. Leslie Weinstein, "DOD Should Use Third-Party Cybersecurity Assessments for Its Vendors," *Federal News Network*, 11 June 2019, https://federalnewsnetwork.com/commentary/2019/06/dod-should-use-third-party-cybersecurity-assessments-for-its-vendors/.
218. Ernie Hayden, "How Supply Chain Security has Evolved Over Two Decades," *Techtarget Network*, November 2018, https://searchsecurity.techtarget.com/tip/How-supply-chain-security-has-evolved-over-two-decades.
219. Hayden, "How Supply Chain."
220. Hayden, "How Supply Chain."
221. Hayden, "How Supply Chain."
222. Hayden, "How Supply Chain."
223. NIST, "New to Framework," accessed 29 March 2020, https://www.nist.gov/cyberframework/new-framework.

224. NIST, "New to Framework."
225. Jennifer Elle and Shaun Khalfan, "The Transition Begins: DOD Risk Management Framework," *CHIPS*, April-June 2014, accessed 29 May 2020, https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=5015.
226. "SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations," *NIST* Computer Security Resource Center, 22 January 2015, http://dx.doi.org/10.6028/NIST.SP.800-53r4.
227. "DOD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs," Defense Acquisition University, January 2017, https://www.dau.edu/tools/Lists/DAUTools/Attachments/140/RIO-Guide-January2017.pdf.
228. Steve Mills and Tim Denman, "The Cybersecurity and Acquisition Life-Cycle Integration Tool," Defense Acquisition University, 28 August 2017, https://www.dau.edu/library/defense-atl/blog/The-Cybersecurity-and-Acquisition-Life-Cycle-Integration-Tool.
229. Ellett and Khalfan, "The Transition Begins."
230. Ellett and Khalfan, "The Transition Begins."
231. Ellett and Khalfan, "The Transition Begins."
232. Ellett and Khalfan, "The Transition Begins."
233. Department of Defense Office of Small Business Programs, "Safeguarding Covered Defense Information—The Basics," accessed 28 May 2020, https://business.defense.gov/Portals/57/Safeguarding%20Covered%20Defense%20Information%20-%20The%20Basics.pdf.
234. Department of Defense Office of Small Business Programs, "Safeguarding Covered Defense."
235. Department of Defense Office of Small Business Programs, "Safeguarding Covered Defense."
236. Department of Defense Office of Small Business Programs, "Safeguarding Covered Defense."
237. Department of Defense Joint Testimony, "Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense," House Armed Services Committee, 21 June 2018, https://docs.house.gov/meetings/AS/AS00/20180621/108468/HHRG-115-AS00-Wstate-BingenK-20180621.pdf.
238. Department of Defense Joint Testimony, "Military Technology Transfer."
239. Department of Defense, *DOD Instruction 5000.02, Operation of the Adaptive Acquisition Framework*, 23 January 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2020-01-23-144114-093.
240. Department of Defense, *Operation of the Adaptive*, 10.
241. Weinstein, "DOD Should Use."
242. Weinstein, "DOD Should Use."
243. Weinstein, "DOD Should Use."

244. Office of the Under Secretary of Defense for Acquisition & Sustainment, "Cybersecurity Maturity Model Certification (CMMC)," accessed 10 April 2020, https://www.acq.osd.mil/cmmc/.

245. Office of the Under Secretary of Defense for Acquisition & Sustainment, "Cybersecurity Maturity Model."

246. Office of the Secretary of Defense Acquisitions, "CMMC FAQ's: Cybersecurity Maturity Model Certification (CMMC)," accessed 23 May 2020, https://www.acq.osd.mil/cmmc/faq.html.

247. Office of the Secretary of Defense Acquisitions, "Cybersecurity Maturity Model Certification (CMMC) Version 1.02," 18 March 2020, https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

248. Wesley Hallman, "NDIA A Perspective: Cybersecurity—Front and Center for Industry," *National Defense*, 6 June 2019, https://www.nationaldefensemagazine.org/articles/2019/6/19/ndia-perspective-cybersecurity---front-and-center-for-industry.

249. Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), accessed April 2021, https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

250. Department of Defense, "Press Briefing by Under Secretary of Defense for Acquisition & Sustain," 31 January 2020, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/.

251. John Harper, "U.S. Allies Considering Adopting Pentagon's CMMC Cybersecurity Standards," *National Defense Magazine*, 4 March 2020, https://www.nationaldefensemagazine.org/articles/2020/3/4/us-allies-considering-adopting-pentagons-new-cybersecurity-standards-for-industry.

252. Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," *Forbes*, 29 April 2020, https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/.

253. Adapted from "Cybersecurity Maturity Model Certification (CMMC) Version 1.02."

254. An advanced persistent threat (APT) is typically are state-controlled malign actors that use continuous, clandestine, and sophisticated intrusion techniques to gain access to a system and remain inside for a prolonged period.

255. "Cybersecurity Maturity Model Certification (CMMC) Version 1.02."

256. "Cybersecurity Maturity Model Certification (CMMC) Version 1.02."

257. "Cybersecurity Maturity Model Certification (CMMC) Version 1.02."

258. CMMC Accreditation Body, "CMMC Accreditation Body," accessed 2 May 2020, https://www.cmmcab.org/.

259. Kendall, "Cybersecurity Maturity Model."
260. Kendall, "Cybersecurity Maturity Model."
261. Kendall, "Cybersecurity Maturity Model."
262. Adapted from Cameron, "What Is the Internet of Military/Battlefield Things (IoMT/IoBT)?"
263. He, et al., "Model of the Product."
264. He, et al., "Model of the Product."
265. Adapted from He, et al., "Model of the Product Development Lifecycle."
266. Melinda Reed, John F. Miller, and Paul Popick, "Supply Chain Attack Patterns: Framework and Catalog," Office of the Assistant Secretary of Defense for Research and Engineering, August 2014, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.6043&rep=rep1&type=pdf.
267. Adapted from He, et al., "Model of the Product."
268. He, et al., "Model of the Product."
269. Reed, et al., "Supply Chain Attack Patterns."
270. He, et al., "Model of the Product."
271. Megan Eckstein, "Navy Needs New Servers for Aegis Cruisers and Destroyers After Chinese Purchase of IBM Line," *USNI News*, 7 May 2015, https://news.usni.org/2015/05/05/navy-needs-new-servers-for-aegis-cruisers-and-destroyers-after-chinese-purchase-of-ibm-line.
272. George Stahl, "IBM Server Sale to Lenovo Passes U.S. Test," *Wall Street Journal*, 15 August 2014, accessed 29 May 2020, https://www.wsj.com/articles/ibm-server-sale-to-lenovo-passes-u-s-test-1408135593.
273. Stahl, "IBM Server Sale to Lenovo Passes U.S. Test."
274. Eckstein, "Navy Needs."
275. Bill Gertz, "Military Warns Lenovo Poses Cyber Spy Threat," *Washington Free Beacon*, 24 October 2016, accessed 29 May 2020, https://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/.
276. Gertz, "Military Warns."
277. Reed, et al., "Supply Chain."
278. Reed, et al., "Supply Chain."
279. He, et al., "Model of the Product."
280. He, et al., "Model of the Product."
281. Craiger and Kessler, "Cybersecurity."
282. U.S. Government General Accountability Office, *Weapons Systems Cybersecurity*.
283. He, et al., "Model of the Product Development Lifecycle."
284. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, 16.
285. Defense Advisory Board Task Force on Cyber Supply Chain, *Report*, 16.

286. Reed, et al., "Supply Chain."
287. He, et al., "Model of the Product."
288. He, et al., "Model of the Product."
289. He, et al., "Model of the Product."
290. Ryan Naraine, "Dell Ships Motherboard with Malicious Code," *ZDNet*, 21 July 2010, accessed 29 May 2020, https://www.zdnet.com/article/dell-ships-motherboard-with-malicious-code/.
291. Chad Perrin, "The Danger of Complexity: More Code, More Bugs," *TechRepublic*, 2 February 2010, https://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/.
292. Perrin, "The Danger of Complexity."
293. Seffers, "Defense Department Awakens."
294. Cameron, "What Is the Internet."
295. Zeljka Zorz, "Malicious Python Packages Found on PyPI," *Help Net Security*, 18 July 2019, https://www.helpnetsecurity.com/2019/07/18/malicious-python-packages/.
296. Dan Goodin, "Malicious Code Added to Open-Source Piwik Following Website Compromise," *Ars Technica*, 27 November 2012, accessed 29 May 2020, https://arstechnica.com/information-technology/2012/11/malicious-code-added-to-open-source-piwik-following-website-compromise/.
297. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*.
298. Chris Stokel-Walker, "A Lazy Fix 20 Years Ago Means the Y2K Bug Is Taking down Computers Now," *New Scientist*, 7 January 2020, accessed 20 May 2020, https://www.newscientist.com/article/2229238-a-lazy-fix-20-years-ago-means-the-y2k-bug-is-taking-down-computers-now/.
299. He, et al., "Model of the Product."
300. He, et al., "Model of the Product."
301. Toohey, "Counterfeit Semiconductors."
302. He, et al., "Model of the Product."
303. He, et al., "Model of the Product."
304. Network routers are special purpose computers that control the information flowing over the internet and are critical to the functioning of the Internet.
305. Tom Espiner, "Cisco Partners Sell Fake Routers to U.S. Military," *ZDNet*, 4 August 2008, https://www.zdnet.com/article/cisco-partners-sell-fake-routers-to-us-military/.
306. Espiner, "Cisco Partners."
307. Espiner, "Cisco Partners."
308. Espiner, "Cisco Partners."
309. Espiner, "Cisco Partners."

310. "RFID Guidance and Reports," *OECD Digital Economy Papers*, no. 50 (2008), accessed 20 May 2020, http://dx.doi.org/10.1787/230334062186.
311. U.S. Government Accountability Office, *Weapons Systems Cybersecurity*.
312. A digital certificate is an electronic document that is used to verify the identity of a company, individual, or server.
313. A certificate authority is an organization or company that validates identities of online entities (e.g., Amazon.com, Apple.com, etc.) and then issues digital certificates to that entity, much like the notary public validates a person's identity by verifying through official government documents such as driver's licenses or passports.
314. Peter Bright, "How the Comodo Certificate Fraud Calls CA Trust into Question," *Ars Technica*, 24 March 2011, https://arstechnica.com/information-technology/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question/.
315. Jack Corrigan, "Supply Chain Attacks Spiked 78 Percent in 2018, Cyber Researchers Found," *Nextgov.com*, 20 February 2019, https://www.nextgov.com/cybersecurity/2019/02/supply-chain-attacks-spiked-78-percent-2018-cyber-researchers-found/154996/.
316. "Software Update Supply Chain Attacks: What You Need to Know," *Threat Intel*, 17 October 2018, https://medium.com/threat-intel/software-update-supply-chain-attacks-what-you-need-to-know-f5bd3ba9718e.
317. Aririf Bacchus, "Secret Backdoor in Asus Update Software Infects Computers with Malware," *Digital Trends*, 27 March 2019, accessed 20 May 2020, https://www.digitaltrends.com/computing/asus-malware-attack/.
318. Jeffrey Esposito, Leonid Grustniy, Sergey Golubev, and Tatyana Sidorina, "ShadowHammer: Malicious Updates for ASUS Laptops," *Kaspersky Daily*, 25 March 2019, https://www.kaspersky.com/blog/shadow-hammer-teaser/26149/.
319. This scenario describes malign actors whose motivation is greed. State-funded malign actors motivation may be to reduce the capabilities of the weapons system.
320. We are not aware of any instance of ransomware as part of a software update occurring as of 2020, yet the possibility exists.
321. "Operating system market share," *Netmarketshare*, accessed April 14, 2020, https://www.netmarketshare.com/operating-system-market-share.aspx.
322. Damien Wilde, "Android Ransomware Is Posing as a Coronavirus Tracking App," *9to5Google.com*, 16 May 2020, https://9to5google.com/2020/03/16/report-android-ransomware-is-posing-as-a-coronavirus-tracking-app/.
323. "Mobile Operating System Market Share Worldwide," *StatCounter Global Stats*, accessed 16 April 2020, https://gs.statcounter.com/os-market-share/mobile/worldwide.
324. From our research it appears that most "ransomware" for the iPhone is "scareware" pretending to be ransomware. The purpose of the scareware is to get the user to pay for removing the malware, even though the malware doesn't actually encrypt the iPhone's files.

325. Lily Hay Newman, "A Scary New Ransomware Outbreak Uses WannaCry's Old Tricks," *Wired*, 27 June 2017, accessed 20 May 2020, https://www.wired.com/story/petya-ransomware-outbreak-eternal-blue/.
326. "Florida City Agreed to Pay $600,000 in Ransom to Hackers," *The Ledger*, 20 June 2019, accessed 20 May 2020, https://www.theledger.com/news/20190620/florida-city-agreed-to-pay-600000-in-ransom-to-hackers.
327. "Florida City Pays $600,000 to Hackers Who Seized Its Computer System," *CBS News*, 20 June 2019, https://www.cbsnews.com/news/riviera-beach-florida-ransomware-attack-city-council-pays-600000-to-hackers-who-seized-its-computer-system/.
328. Lawrence Abrams, "Ransomware Attacks Prompt Louisiana to Declare State of Emergency," *BleepingComputer*, 25 July 2019, https://www.bleepingcomputer.com/news/security/ransomware-attacks-prompt-louisiana-to-declare-state-of-emergency.
329. Ionut Ilascu, "'Coordinated Ransomware Attack' in Texas Hits 23 Local Governments," *BleepingComputer*, 18 August 2019, https://www.bleepingcomputer.com/news/security/coordinated-ransomware-attack-in-texas-hits-23-local-governments/.
330. Federal Bureau of Investigation, "2019 Internet Crime Report."
331. Josephine Wolff, "The Real Reasons Cybercrimes May Be Vastly Undercounted," *Slate Magazine*, 12 February 2018, https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html.
332. Conner Forrest, "Cloud Diversity: How 10 Companies Use the Cloud 10 Different Ways," *TechRepublic*, 16 November 2016, https://www.techrepublic.com/article/cloud-diversity-how-10-companies-use-the-cloud-10-different-ways/.
333. Heidi Peters, "DOD's Cloud Strategy and the JEDI Cloud Procurement," *U.S. Library of Congress*, Congressional Research Service, 13 November 2019, https://crsreports.congress.gov/product/pdf/IF/IF11264Equipment.pdf.
334. Department of Defense, "DOD Cloud Strategy—U.S. Department of Defense," accessed 24 April 2020, https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF.
335. "Armor Detects and Neutralizes 681 Million Cyberattacks," *Armor.com*, 23 January 2019, https://www.armor.com/resources/armor-detects-neutralizes-cyberattacks/.
336. Critical systems are normally taken offline when updates are required. Patches are applied, and then the systems are tested to ensure that the update has not caused any problems. Only then is the system put back into service.
337. He, et al., "Model of the Product."
338. He, et al., "Model of the Product."
339. CDs and DVDs require physical destruction to ensure information cannot be read.

340. Philip Craiger, "Computer forensics methods and procedures," *Handbook of Information Security* Vol 2., ed. Hossein Bigdoli (New York: John Wiley and Sons, 2006), 736–55.
341. Craiger, "Computer forensics," 736–55.
342. File metadata would include file name, file size, file location, permissions, type of file, etc.
343. There are other ways of securely deleting files from magnetic media—such as degaussing, which removes all the magnetic information from a mechanical hard drive. However, this equipment is not readily available to the average user.
344. Paul Burke and Philip Craiger, "Trace Evidence of Secure Delete Programs," in *Advances in Digital Forensics II* eds. Martin Olivier and Sujeet Shenoi (New York: Springer, 2006), 185–98.
345. The NSA provides guidance on the sanitization of media containing classified information, including degaussing, physical disintegration of the media into particles that are nominally 2-millimeter edge length in size, or incineration, reducing the devices to ash.
346. Joe Capobianco and David Phillips, "Strengths and Myths of What Makes Special Operations Forces Acquisition Special," 14 May 2018, https://www.army.mil/article/205259/strengths_and_myths_of_what_makes_special_operations_forces_acquisition_special.
347. Capobianco and Phillips, "Strengths and Myths."
348. "Special Operations Forces Acquisition, Technology, and Logistics," *SOF AT&L*, accessed 23 March 2020, https://www.socom.mil/SOF-ATL.
349. "Our organization," *SOF AT&L*, accessed 15 February 2021, https://www.socom.mil/SOF-ATL/Pages/Our-Organization.aspx.
350. "Our organization," *SOF AT&L*.
351. Capobianco and Phillips, "Strengths and Myths."
352. "Our organization," *SOF AT&L*.
353. "Press Briefing by Under Secretary of Defense for Acquisition & Sustainment, para 21.
354. "Other Transactions (OT) Guide—DAU," *Defense Acquisition University*, November 2018, accessed 15 May 2020, https://www.dau.edu/tools/t/Other-Transactions-(OT)-Guide.
355. "Other Transactions (OT) Guide—DAU."
356. "Other Transactions (OT) Guide—DAU."
357. Scott Maucione, "As OTAs Grow, Traditional Contractors Are Reaping the Benefits, *Federal News Network*, 5 November 2018, https://federalnewsnetwork.com/contracting/2018/07/as-otas-grow-prime-contractors-are-reaping-the-benefits/.
358. "Next Generation Information and Identification Awareness (NGIA) Capability Assessment Event," SOFWERX, 20 June 2019, https://www.sofwerx.org/ngia/.

359. "SOFWERX," SOFWERX, accessed 14 May 2020, https://www.sofwerx.org/faqs/.

360. "Innovation Foundry Event (IF5)," SOFWERX Discover, accessed 14 May 2020, https://www.sofwerx.org/discover/.

361. "SOFWERX."

362. "Science and Technology Small Business Innovation Research (SBIR) 20.1," *SOFWERX Discover*, accessed 24 May 2020, https://www.sofwerx.org/discover/.

363. "Science and Technology Small Business Innovation Research (SBIR) 20.1."

364. Department of Defense, "Cybersecurity and Acquisition Lifecycle Integration Tool (CALIT)," Defense Acquisition University, accessed 23 May 2020, https://www.dau.edu/library/defense-atl/blog/The-Cybersecurity-and-Acquisition-Life-Cycle-Integration-Tool.

365. CALIT incorporates different instructions and policies, including *DODI 500.02, Operation of the Defense Acquisition System, Encl 14 (Cybersecurity in the Defense Acquisition System)*; *DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), Cybersecurity Test and Evaluation, Program Protection, and System Security Engineering (SSE), Cyber Threat Analysis*; *DODI 5200.39, Critical Program Information Identification and Protection Within Research, Development, Test and Evaluation*; and *DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks.*

366. Department of Defense, "DOD Cybersecurity Chart: Build and Operate a Trusted DODIN," DOD Information Analysis Center, accessed 19 April 2020, https://dodiac.dtic.mil/dod-cybersecurity-policy-chart/.

367. Department of Defense, "DOD Cybersecurity Chart."

368. Department of Defense, "DOD Enterprise DevSecOps Reference Design," Chief Information Officer, 12 August 2019, https://dodcio.defense.gov/Portals/0/Documents/DoD Enterprise DevSecOps Reference Design v1.0_Public Release.pdf?ver=2019-09-26-115824-583.

369. Department of Defense, "DOD Enterprise."

370. Lauren C. Williams, "DOD Plans for Security-Focused Guidance for DevSecOps," *FCW*, 23 January 2020, https://fcw.com/articles/2020/01/23/dod-devsecops-guidance-williams.aspx.

371. Department of Defense, "DOD Enterprise DevSecOps."

372. Department of Defense, "OSD DevSecOps Best Practice Guide," Defense Acquisition University, 15 January 2020, https://www.dau.edu/cop/it/DAU%20Sponsored%20Documents/DevSecOps_Whitepaper_v1.0.pdf.