AU/ACSC/2015

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

PROACTIVE DEFENSE FOR EVOLVING SUPPLY CHAIN COUNTERFEITING

by

Michael J. Blair, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisors: Dr. Richard Smith

Dr. Heather Marshall

Maxwell Air Force Base, Alabama

December 2015

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Contents

DEFINITION OF TERMS

The following terms are used throughout this study.

Advanced persistent threat (APT): a cyber-attack that utilizes multiple vulnerabilities to break into a system, avoids advanced detection techniques, and acquires data or disrupts operations.[1]

Blacktopped: previously used parts that counterfeiters make to look new by sanding original markings down and remarking them with new vendor labels or stamps.[2]

Counterfeit part: a part that has been copied without a legal right of authority by the patent owner; an unauthorized fake or knock off part that is misrepresented by a supplier in the federal supply chain; a previously used part that is made to look as new and is sold as a new part. [3]

Elongated or multi-tier supply chains: using multiple primary supply chain sources to reduce manufacturing costs.

E-Waste: electronic waste that has been discarded as trash and is sold to counterfeiters who reprocess the parts and sell them as original products.[4]

Information Communication Technology (ICT): refers to the information and communications technology (software and hardware) that enables cyber space domain communications.[5]

Insider Security Threat: an outside entity that poses to be a legitimate ICT resource and resides within the internal enterprise network as an insider with access to the organization's processes, data and computer systems.[6]

National Security System (NSS): Title 44 §3532 defines national security system as "…any information system used or operated by an agency or by a contractor of an

agency, which: (A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) is critical to the direct fulfillment of military intelligence missions.[7]

Non-National Security System (NNSS): a system that is used to support routine administrative functions such as human resources, logistics, finance, and payroll.[8]

Original Equipment Manufacturer (OEM): refers to the company that originally built a product.[9]

Supply Chain Risk: risks that arise from the confidentiality, integrity, or availability of information systems and reflect the potential adverse impact to organizational operations, organizational assets, individuals, other organizations, and the nation.[10]

White Hat Hacker: an ethical computer security expert who specializes in offensive attacks and utilizes these skills to ensure the security of ICT.[11]

ACKNOWLEDGEMENTS

I dedicate this work to family members who provided support, guidance, advice, motivation, time, and patience over many decades of my pursuit of higher education. My mother provided the foundation for my morals and values that has guided me throughout my life. Today she continues to express pride and support as I report on the work reflected here.

To my daughters, you are and will always be my personal inspiration to be successful and well-grounded on the important things in life. Thank you for your admiration, love and continued support, allowing me time to chase my educational goals.

Most importantly, I dedicate this work to my wife, who has stood by me with support, encouragement, and advice through four different graduate schools spread across 22 years of marriage. For the past few years, she has endured a life with an "absentee husband" who hid in the study on nights and weekends, has advised me on writing quality, taken on extra work in the house, and kept me focused on what is important in life.

ABSTRACT

The past decade has seen an increase in the development of proactive cyber defense methods that focus on anticipated future attack strategies and are integrated into the cyber defense designs. The historic co-evolution of the attacker (counterfeiter) and defender (USAF) provide a conceptual understanding on how policy has failed to adequately reduce the security risks that counterfeit electronic parts present to advanced weapon systems. The first part of this study provides the background and history of counterfeit electronics within the Unites States Department of Defense (DOD). The second part of the study provides the current political, economic, social, technological and military analyses on electronic counterfeiting threats, risks and mitigation strategies associated with this phenomenon. The research concludes with a discussion on why the following four recommendations are needed to effectively mitigate the threat and associated risks: (1) Increase funding to ensure anti-counterfeiting practices are built into weapon system designs and manufacturing; (2) Support the reclassification and treatment of counterfeit electronics as a cyber-security insider threat; (3) Increase threat awareness for leaders to effectively implement deterrence policy and strategies; (4) Develop a proactive anti-counterfeiting framework that leverages predictive analytics modeling and computational criminology.

INTRODUCTION

The Air Force (AF) has invested billions of dollars on research and development (R&D) to create the most technologically advanced and superior military force in the world and will continue to face challenges when trying to develop and sustain technologically advanced weapon systems. The safety of our military men and women is dependent on the performance and reliability of incredibly sophisticated technology components. Due to globalization, technology supply chains are challenged by and/or plagued with businesses trying to meet the increasing demands for sophisticated and mature technologies. The use of extended supply chains by DOD contractors increases the likelihood that suppliers beyond the primary contractor could compromise supply chain security.

In 2011, the Senate Armed Services Committee conducted an investigation into the DOD's supply chain processes and the potential for counterfeit electronic parts integration in advanced weapon system programs.[12] The outcome of the investigation exposed that the defense supply chain utilized hundreds of un-vetted manufacturers, including China, to supply electronics on sensitive defense systems. [13]

Some critics argue, however, that it is challenging, if not impossible, to identify counterfeit products from the potential thousands of resistors, microprocessors and semiconductors used to assemble a weapon system.[14] Regrettably, without anti-counterfeiting processes that inspect or analyze products carefully, the potential for weapon system failure increases dramatically.[15] This research will focus on developing a new dynamic supply chain defense framework that will provide a proactive approach to actively identifying supply chain threats and creating a comprehensive response to

suspect counterfeiting attacks. Developing new countermeasures and improving corporate acquisition processes will help ensure the integrity of AF weapon systems, increase the safety and security of our military personnel, and save billions of dollars lost each year to cyber security attacks.

BACKGROUND

Security concerns over supply chain counterfeiting and malicious cyber hardware attacks have prompted a number of congressional investigations. Subsequently, these inquiries produced relevant research works that have added value to the overall cyber security body of knowledge and supply chain risk management areas. Although most literature on these topics focuses on a reactive technical solution, the researcher's conclusions will be to develop a predictive supply chain defense framework that encompasses a proactive defensive approach to actively identify and mitigate supply chain threats.

Traditional approaches in supply chain risk management are inadequate against today’s increasingly sophisticated supply chain attacks, as evidenced by research related to this topic. [16] Arati Prabhakar, Director of the Defense Advanced Research Projects Agency (DARPA) understands that a reactionary approach to fixing the cyber security issues is not working.[17] The complex and often multi-tiered defense supply system is a difficult problem to isolate and systematically study to provide a solution.[18] Lamb, Ling and Hayes explain that dynamic cyber defense provides an integrated enterprise approach towards creating multiple layers of defense within a system.[19] Each layer of the system serves to mitigate or reduce the threat and overall business risk.

Filsinger, Fast, Wolf, Payne, and Anderson have recognized that the outsourcing

of defense technologies by the U.S. and its dependence on foreign technology has created a supply chain vulnerability that is decreasing AF technological advantages in many areas.[20] Additionally, the acquisition of technologies both inside and outside of the U.S. to support mission critical systems increases our vulnerabilities because there is no foolproof method that can detect inferior components or counterfeit hardware.[21]

Counterfeiting is one of the fastest growing economic crimes of modern times and threatens the very fabric of our national security. [22] This criminal empire knows no boundaries and continues to affect businesses, consumers and government agencies around the world. Today, the International Chamber of Commerce estimates that counterfeit products, valued at $600 billion annually, account for approximately 5 - 7% of world trade.[23] There is considerable concern within the federal contracting community about the infiltration of counterfeit parts into the government supply chains. The ever-increasing reliance on global supply sources exposes the federal supply systems to an enlarging risk of exploitation via counterfeit materials, malicious software and untrustworthy electronic products.[24]

A Senate Armed Services Committee inquiry, that spanned 2009-2010, revealed an abundance of counterfeit products from China in the DOD supply chain. Over the course of the investigation, The Committee found that more than one million electronic parts were suspected to be counterfeit.[25] In 2010, the committee's investigation found that L-3 Display Systems bought memory chips from an electronics distributor in California that were purchased from Hong Dark Electronics Trade, a company in China. The memory chips were used in display systems installed on the Air Force C130J and C-17 aircrafts that provide the pilot with information on the operation of the aircraft, such as

engine status, altitude, airspeed, location and navigation messages.[26] Further investigations by the AF revealed, "…approximately 84,000 suspect counterfeit electronic parts purchased from Hong Dark entered the DOD supply chain, and many of these parts have been installed on DOD aircraft."[27]

PURPOSE

The intent of this problem solution study is to explore the illicit electronics counterfeiting industry and analyze how counterfeit electronics are acquired through the federal government supply chain, and subsequently installed in advanced weapon platforms in the United States Air Force. The focus will be on how the current Department of Defense supply chain risk model is ineffectual due to the misclassification of counterfeit electronics as an economic crime; the lack of support and funding by senior leaders; and that the reactionary nature of the model prevents a proactive cyber response and deterrence.

RESEARCH METHODOLOGY

The literature review process began with those same three general topic areas, then narrowing the search down to more specific search topics as the literature search progressed. The goal was to understand the current security issues associated with global supply chains and their association with Air Force weapon system programs.

Citation chaining will be utilized to develop a broad exploratory analysis of available academic resources.[28] As part of this research, an examination of scholarly peer reviewed journals, congressional reports, testimony, and legislation will be studied in

addition to international industry standards. The organization of the literature review will provide a historical analysis to show familiarity with current initiatives and technological developments. Analysis of research reports provided by Washington Think Tanks will ensure current DOD programs are evaluated for efficacy and security considerations. Additional analysis provided by the National Institute of Technology (NIST), Armed Forces Communications and Electronics Association (AFCEA) and the Institute of Electrical and Electronics Engineers (IEEE) will be studied to provide an industry-wide review of technology supply chain best practices, security vulnerabilities and their effects on Air Force weapon systems.

The literature for the study was drawn from the following available open source online databases: Science Direct, IEEE Xplore, ACM Digital Library, ProQuest, EBSCO Host, SAGE Journals, and Google Scholar. Each of these databases were searched sequentially with a series of search terms or phrases: supply chain security, DOD acquisition supply chain, counterfeit electronics, global supply chain counterfeit security concerns, secure global supply chains, proactive approach to cyber security, dynamic cyber defense, cyber security in supply chain, supply chain forensics, predictive analytics, security informatics, computational criminology. In addition, use of citation chaining enabled discovery of additional relevant academic literature.[29]

The researcher will use a pragmatic worldview to study the problem of counterfeit electronics in AF weapon systems. Pragmatism encourages the use of multiple research methodologies, different worldviews and different forms of data collections.[30] Using a qualitative research design and a problem-based research approach will postulate a philosophical basis to study a current technological security concern and provide

recommended solutions for reducing risk exposure of this phenomenon. The intent of the qualitative research will provide a framework for the researcher to compare and contrast how the cyber security framework and the supply chain risk management framework can be combined to develop a comprehensive approach to reducing the risk of counterfeit parts and sophisticated electronics acquisition into the federal supply system.

LITERATURE REVIEW

Political Importance

Over the last 25 years, the U.S. Government has conducted numerous studies to establish national policies and organizational structures that would guide the activities needed to protect national security systems. During the course of the 99th Congress (1985-1986), the American Bar Association, the Inspector General's Office of the Department of Health and Human Services, and computer crime experts noted that the lack of management, controls, and coordination of computer security in the both the private and government sectors is alarming.[31] "One of the most disturbing findings from this study is that the work environment provided the perpetrators with the opportunity to commit their crimes," the Chairman of the President's Council on Integrity and Efficiency investigating computer crime, said when he testified on October 29, 1985.[32]

In response to the findings by the 99th Congress, the House Science and Technology Committee requested that the U.S. Government Accountability Office (GAO) review whether security controls were being assimilated into mission-critical and sensitive systems that were developed by federal civilian agencies. Thomas B. Giammo, Associate Director, Information Management and Technology Division of GAO, testified

that out of the nine civilian agencies who were audited, all failed to assure appropriate security controls were incorporated into the development of mission-critical or sensitive systems.[33] As a result of the 99th Congress testimonies and GAO findings, the 100th Congress passed H.R. 145, The Computer Security Act of 1987.

H.R. 145 provided the federal government a framework that helped provide direction to the mixture of laws, regulations and responsible agencies regarding cyber security.[34] The bill's main focus was securing the information or data stored in federal computer systems.[35] Although this bill did not directly offer strategies for preventing counterfeiting, it did provide the foundation for educating users on cyber security related issues and designated the National Institute of Standards and Technology (NIST), formerly the National Bureau of Standards (NBS), as the focal point within the government to develop computer security standards and guidelines for systems other than NSS.[36]

In 2008, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI) under the National Security Presidential Directive 54 (NSPD) 54 and Homeland Security Presidential Directive 23 (HSPD) 23. The purpose of these initiatives was to provide federal and state agencies with strategies, source intelligence community vendor threat information, and guidance on how to secure cyberspace.[37] Building upon the CNCI enacted by President Bush, President Barrack Obama characterized cyber security as "…. one of the most serious economic and national security challenges we face as a nation" and ordered a thorough evaluation on how to better defend the U.S. Information and Communication Technology (ICT) infrastructure.[38]

Initiative Eleven of the CNCI recognizes the need to develop a "multi-prong approach" to solving supply chain risk management concerns.[39] The goals of this approach will assist domestic and global supply chain with reducing the risks, threats, and vulnerabilities; consequences of poor acquisitions decisions; development of tools and mitigating techniques; new acquisition processes and practices that reflect the dynamic global marketplace; and develop partnerships with industry to institute supply chain risk management (SCRM) standards and best practices to help reduce risks across the lifecycle of product development.[40]

In 2011, Section 818, Public Law 112-81 (National Defense Authorization Act, FY 2012) mandated into law a requirement for the DOD to conduct an assessment of the current acquisition practices and policies. The law required the DOD to develop an inspection program that would detect and avoid counterfeit electronic parts.[41] In response to the NDAA, the DOD issued DOD Instruction 4140.67 (DODI 4140.67), DOD Counterfeit Policy, which established a counterfeit prevention policy.[42] DODI 4140.67 provided a broad policy on supply chain counterfeiting and delivered more informing and assigning, than actually instructing. For example, the instruction does not provide guidance on how to implement federal controls on suppliers nor does it explain how it will hold contractors accountable for detecting and avoiding counterfeit parts.

Economic Impact Analysis

The Report to Congress on Foreign Economic Collection and Industrial Espionage investigation revealed that "sensitive U.S. economic information and technologies" are the target of intelligence services and private sector companies from a dozen foreign countries.[43] The DOD Director of Operational Test and Evaluation states,

"Poor reliability is a problem with major implications for costs…Poor reliability leads to higher sustainment costs for replacement spares, maintenance, repair parts, and facilities".[44] The U.S. government needs to take a more comprehensive approach to supply chain risk management (SCRM) by developing a better understanding on how commercial suppliers can ensure the integrity and fidelity of their products and services.[45] The acquisition and utilization of counterfeit and fake technology parts will have devastating or catastrophic impacts on mission critical systems or advanced DOD weapon systems.[46]

Research has shown that in addition to national security risks, counterfeit electronics increase the cost of defense systems.[47] The Budget Control Act of 2011 is continuing to constrain the Air Force's ability to effectively plan and afford advanced weapon systems. The DOD's Comptroller states that weapon system programs need to maintain a "…buying only the cost-effective parts needed to accomplish the mission" approach and that program managers need to continue to evaluate cost versus value.[48] This guidance is in direct conflict of what the Senate Armed Services Committee (SASC) recommended as part of the inquiry and found that counterfeit electronic parts pose long-term sustainment problems, which is a major driver for the overall cost of the system.[49]

The DOD Comptroller released the budget request for the AF that is well under the required amount to achieve mission strategy in FY2016. The 2016 Department of Defense Budget request identifies increased spending for Science and Technology of $12.3 billion, and $84.1 million for Defense Acquisition Workforce Development Fund (DAWDF).[50] Sequestration will continue to challenge the acquisition and development of superior weapons for the foreseeable future. These fiscal challenges will force military

research and development toward a less desirable weapon technology or force them to purchase fewer weapons to ensure the integrity of design and implementation of the weapon program.

The GAO report identified that the main issues on the developing advanced weaponry is the forced utilization of immature technologies in advanced weapon systems.[51] The upfront costs of products acquired through authorized sources are typically higher than those electronic components marketed on the open economy.[52] These practices include sole-sourcing, outsourcing and global sourcing of supply chain vendors. A Rand report on the AF identified these practices as being effective but also recognized that having fewer supply sources creates a strategic risk because the overreliance on a sole source could potentially affect the overall design and performance of the supply chain system.[53]

The U.S. government is financially unable to develop and manufacture the technological industrial base needed to sustain research and development of weapons. Our dependency on foreign technology manufacturing creates ample opportunities for intentional compromise of ICT components while they are being created, assembled, and delivered throughout the supply chain. Introducing immature technology into an advanced technology weapon system is concerning due to reliability concerns and sustainment operations, which account for almost two-thirds of the overall life cycle costs of major weapon systems.

Congressional testimony reported that the theft of U.S. Intellectual Property Rights (IPR) by Chinese counterfeiters is creating significant national security vulnerabilities as well as severely impacting our economic security.[54] There are about

200,000 semiconductor manufacturing employees in America and counterfeiting operations put these jobs at risk as well as jeopardizes the American jobs yet to be created.[55] The Semiconductor Industry Association (SIA) estimates that global counterfeiting operations cost the U.S. manufacturers about $7.5 million in lost revenue and subsequently 11,000 U.S. jobs. In April 2012, an industry market research firm (HIS iSuppli) reported that the five most prevalent types of counterfeit products used by commercial and military industry (transistors, analog integrated circuit (IC), microprocessor IC, memory IC, and programmable logic IC) represent $169 billion in potential annual risk to global electronics supply chains.[56]

The estimated annual revenue lost due to ICT counterfeiting is a staggering $100 billion each year.[57] Notably, this dollar figure only accounts for the losses associated with counterfeit electronics and does not account for the repair or maintenance costs required to repair defective-bogus parts.[58] For example, the Armed Services Committee investigation uncovered that the Missile Defense Agency (MDA) computers responsible for Terminal High Altitude Area Defense (THAAD) missiles contained suspected counterfeit memory devices.[59] This cost the taxpayer $2.7 million to fix the issue.

Social Impact Analysis

Semiconductors have had a tremendous impact on our society. Mission critical ICT systems rely on semiconductors to provide the “brains” to power hardware application that are found in healthcare, supervisory control and data acquisition (SCADA), automotive braking, and military and aerospace systems. Because they are integrated into these vital ICT electronic systems, counterfeit semiconductors create a huge risk to the health, safety and security of people worldwide. For example, a broker

shipped counterfeit semiconductors that were going to be installed in radiation detectors used by first responders during a nuclear accident.[60]

The majority of the ICT infrastructure and manufacturing capabilities are largely owned by both national and international small and large businesses. To adequately address the cyber security concerns related to supply chain counterfeiting and theft of intellectual property, a domestic and international partnership is needed.[61] Equally important is developing a comprehensive cyber security response that will deter counterfeiting operations from reaching U.S. supply chains and ultimately protect the U.S. citizens and military from the national security threats created by counterfeit and substandard products.[62]

Cyber-attacks against the U.S. have increased in sophistication and severity due to the technological interconnectedness that globalization has provided. U.S. Cyber Command (CYBERCOM) estimated that there are approximately 250,000 probes or attacks every hour, or more than six million a day against U.S. government networks .[63] An estimated three billion people use the Internet daily and another 4.9 billion devices are connected to the Internet – a phenomenon known as the Internet of the Things (IoT).[64] It is estimated that by 2020 the number of IoT connections will be in the excess of 25 billion devices.[65]

The ICT domain is a critical element for business success and mission accomplishments. It provides the cutting edge technologies that ensure the U.S. military sustains advanced weapons superiority. The federal acquisition concern is the continued reliance on foreign technology firms to support our procurement and development of advanced weaponry. Adversaries have recognized the U.S. military's constant demands

for advanced technology in the midst of narrowing global supply sources. This supply deficiency provides an attack vector to compromise our critical systems with counterfeit products or substandard semiconductors and microprocessors. Other than malicious intent, supply chain counterfeiting is operated by foreign state actors who are trying to degrade the technological advances of the US defense industrial base. The Senate Armed Service Committee found China as the dominant source country for counterfeit electronics that are infiltrating our DOD supply systems.[66]

To try and improve the U.S.-China relations and garner international support to end the prevalent counterfeiting industry in Mainland China, the SASC requested the Chinese Ambassador approve a U.S. envoy to survey the vast counterfeiting industry. Although repeated requests were made to the Chinese Ambassador and other senior diplomats in Hong Kong and Beijing, the committee's staff was denied entry. As a result of the Chinese Government's reluctance to help the committee's investigation, Senator Carl Levin stated the U.S. should "…. treat all electronic parts from China as suspect counterfeits."[67]

The ICT semiconductors industry spends tens of billions of dollars to research, engineering, development and manufacturing to ensure the products provided operate reliably.[68] Counterfeiters utilize poor manufacturing techniques to copy stolen IP products resulting in original component manufacturer's reputation being damaged. More importantly just one counterfeit semiconductor has the capability to make an entire critical system to fail and cause catastrophic damage or even death.

Technological Analysis

The unclassified U.S.-China Commission describes China's capabilities to

conduct advanced cyber warfare and computer network exploitations (CNE) through malicious cyber operations that are often undetected by their targets.[69] Historically the defenses of cyberspace networks utilized a reactionary intrusion detection approach to prevent ICT attacks, such as malicious software propagation and network intrusions. Using industry best practices for cyberspace security, cyber security analysts (white hat hackers, red teams) are proactively scanning physical and logical enterprise entry/exit points to identify any security vulnerabilities within the AF networks. Understanding that targeted CNE operations are successful, cyber security personnel are able to conduct proactive scanning operations to identify potentially harmful malicious code within the AF networks.

The complexity and anonymity of the internet provide adversaries with a safe haven to conduct pervasive cyber-attacks aimed at industrial espionage. Similarities between exploitation tools and tactics among nation state attackers are making it harder to attribute cyber intrusions.[70] The increase in non-attribution could be related to the wide spread availability and use of open source malicious software, network exploitation tools, and commercial anonymity services. The decrease in reported incidents may also be due to the intelligence communities concern with attribution being overshadowed by the private sector's desire to prevent certain of types of cybercrime.

The process to engineer a trusted electronics component requires a significant investment in time and money to protect the product from compromise and ensure the overall integrity of the weapon system. The Air Force Research Laboratory (AFRL) requires that hardware and software-intensive systems demonstrate an appropriate level of maturity before they can be introduced into a weapons program.[71] As a result of the

long AFRL's development stages, DOD contractors are more likely to use commercial technology supply chains to fill the void of mature DOD technologies thereby increasing the chances of receiving counterfeit electronics.

The fidelity and integrity of sophisticated technology relies upon a trusted DOD procurement process. However, due to globalization and the demand for mature technologies, the federal supply chains capable of providing sophisticated and trusted technologies are narrowing. As a result, U.S. defense contractors who are unable to afford the mature technology components manufactured within the U.S. may unknowingly purchase substandard materials and parts from third party suppliers or foreign competitors to avoid costly contract overruns. This federal contracting approach increases the chances of counterfeit or substandard technology entering the AF supply chain.

Military Analysis

The national security concerns regarding counterfeit electronics installed in advanced weapon platforms are well documented by numerous Congressional Committee Investigations, Scientific Communities, and independent researchers. Counterfeit electronics have been found installed in C-130J, C-17, C-27J, P-8A Poseidon, AH-64 military aircraft, as well as the computers that control the Terminal High Altitude Area Defense (THAAD) missile. Subsequent to these findings, industry best practices were compiled and instituted by the United States Federal Supply Chain system to reduce the security risks. Within the ICT community, the current supply chain risk management framework, developed and instituted by the National Institute of Standards and Technology (NIST), uses a reactionary approach to reducing counterfeit electronics. As

new counterfeiting techniques are discovered, the Federal Acquisition Regulation (FAR) System creates defensive security controls to identify and respond. There is an immediate concern for military leaders and weapon system manager to increase the awareness on this threat to ensure adequate security is in place.

Nation States: Sources of Counterfeits

The Office of the National Counterintelligence Executive (ONCIX) states, "Chinese actors are the world's most active and persistent perpetrators of economic espionage."[72] China was the number one source of counterfeit products seized on the U.S. border in 2014.[73,74] It is estimated that 20 percent of consumer products in the Chinese market are suspected as counterfeit. The complexity and diversity of the federal ICT supply chain provides significant opportunities for the insertion of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software and hardware.[75] There is also the threat of trade secret thefts, which can occur when employees leave the company with portable storage devices containing proprietary information, cyber intrusions, and failed joint ventures.[76]

Senator Carl Levin, Chairman, Committee on Armed Services, testified that the investigation into the DOD supply chain revealed that each of the defense contractors and ICT brokers interviewed all pointed toward China, specifically the City of Shenzhen in Guangdong Province as the primary source of counterfeit electronic parts.[77] In March 2015, the United States Trade Representative (USTR) created a "Notorious Markets List", detailing the worst markets that sell counterfeit goods. The report noted that China remains one of the primary distribution channels for pirated and counterfeit goods in much of the world.[78] This report also provides the U.S. and foreign governments with a

prioritized list of IPR enforcement areas around the world.

Pursuant to Section 182 of the Trade Act of 1974, and as amended by the Omnibus Trade and Competitiveness Act of 1988 and the Uruguay Round Agreement Act (19 U.S.C. § 2242), the Special 301 Report is conducted annually to review the status of the intellectual IPR protection and enforcement in the U.S. and around the world.[79] The purpose of the report is to encourage and sustain adequate and effective IPR enforcement worldwide and captures a range of concerns including: (a) deterioration in IPR protection; (b) inadequate trade secret protection in China, India and elsewhere; (c) online copyright piracy in countries such as Brazil, China, India, and Russia.[80]

Counterfeit Parts Interdiction Efforts

President Obama announced the creation of the Interagency Trade Enforcement Center (ITEC) during his 2012 State of the Union address.[81] The purpose of the ITEC is to provide a whole-of-government approach to protecting and enforcing American trade rights around the world. A primary concern with current anti-counterfeiting efforts is the dynamic nature of counterfeiting techniques. As anti-counterfeiting tools are developed, the counterfeit supplier has already changed its attack vector to circumvent mitigating operations.[82] Counterfeiting and piracy trends listed in the 2015 Special 301 Report, identify that preventive measure are often thwarted because counterfeiters are using legitimate mail, international couriers, and postal services to deliver counterfeit and substandard goods.[83] Effective border control and enforcement at the borders will help prevent the exportation and flow of counterfeit products from the country of origin.[84]

DOD electronic suppliers suggest that if the electronic component passes the contractor implementation test than the part should be considered new and not suspect to

counterfeit. However the original manufacturer and DOD leaders argue that this is not the case and electronic suppliers should be held liable for any maintenance or replacements.[85] An identified problem is waste electronic parts that are discarded for recycling are being repackaged and sold as new products. Counterfeit parts can also be parts that have been used, discarded and repackaged as a new electronic product.

In Fiscal Year 2014, U.S. Customs Border Patrol and the General Administration of China Customs (GACC) conducted joint IPR enforcement operations to interdict shipments of consumer electronics. Although the Chinese government is ramping up efforts to curtail Mainland counterfeiting operations, it is estimated that almost 63 percent of the IPR infringing products were seized at U.S. ports in Fiscal Year 2014; 25 percent transshipped from Hong Kong.[86]

Open source U.S. Intelligence report that the Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), is conducting a range of activities to "…collect economic information and technology from U.S. targets."[87] A majority of Russian Intelligence counterfeiting efforts, includes, but is not limited to online piracy and trademark counterfeiting. The Special 301 Report investigations revealed that Chinese-origin electronic counterfeit products are shipped unrestricted from the Kazakhstan-China border and through Kyrgyzstan, into Russia.[88]

Predictive Analytics and Computational Criminology

"We must avoid out historical pattern of drawing down too fast and getting too small, especially since our record of predicting the future has not been very good. As we make difficult resource decisions, we must be thoughtful in understanding the risk we incur to our nation's future security" General Raymond Odierno[89]

The ability to predict future attacks and outcomes provides a significant strategic operational advantage for military leaders and planners. Effectively, this approach is

already in use by law enforcement and cyber security analysts who utilize predictive analytics to compute the possibility of certain types of crime and cyber-attacks. Using intelligence information and crime statistics from known or past events criminologists and security analysts are able to predict future attacks and proactively establish a formidable targeted counter defense.

Organizations that have already implemented statistical defense based systems understand that this defense approach is not immediate and requires a significant amount of resources to compile the variables and empirical data needed to develop a functional predictive analytics model.[90] By using predictive analytics, organizations are capable of identifying internal and external threats by creating independent risk calculations and detecting deviations from the norm.[91]

The AF Office of Scientific Research (OSR) is currently researching the discovery of mathematical laws that leverage reliable and robust algorithms and human machine decision making to develop accurate real-time projections of the dynamic battle space.[92] For example, the Computational Cognition and Machine Intelligence area is focused on developing innovative research using high-order cognitive processes that will help increase human performance during complex decision making.

RECOMMENDATIONS

Recommendation-1: The cost of doing business

The current DOD anti-counterfeiting approach as described and documented in DODI 4140.67, DOD Counterfeit Prevention Policy, and NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, where the risk management frameworks both suggest a reactionary approach to responding to

electronic counterfeiting incidents. The ICT SCRM provides guidance on how the federal government should implement SCRM at all levels. ICT SCRM includes all activities related to weapon system development lifecycle, such as research and development, and disposal and retirement of ICT equipment (software and hardware).

The ICT SCRM framework builds on the four pillars of cyber security: security, integrity, resilience, and quality, which are the fundamental attributes that must be present to effectively manage supply chain security. The security supply chain encompasses the security triad (confidentiality, integrity, and availability (CIA)). Integrity protects information, systems and services from unauthorized modifications and ensures that supply chain products are genuine and will perform according to documented manufacturer specifications. Resilience ensures that ICT supply chain products will remain available during stress of failure. Quality helps reduce the vulnerabilities that may lead to system or component failure and provide exploitation capabilities.

Understandably there will be costs associated with federal risk mitigation techniques but the concern is that the risk is being offset to the men and women in uniform in addition to jeopardizing our national security. The implementation of the NIST 800-161 ICT SCRM framework involves increased cost due to required changes in manufacturer product development and oversight. Regrettably, the guidance provided by the NIST 800-161 framework does little to enforce the best practices. Similarly, DOD 4140.67 guidelines only instruct supply chain acquirers on how to reduce supply chain counterfeiting but fail to actually enforce compliance. For example, the NIST 800-161 states, “Acquirers should evaluate and weigh the costs of adding ICT SCRM requirements into agreements against the risks to organizations of not adding ICT SCRM

requirements". [93] This guidance is counterintuitive to Public Law 112-81, National Defense Authorization Act for Fiscal Year 2012, that requires DOD Contractors at all tiers be responsible for "….detecting and avoiding the use or inclusion of counterfeit electronic parts" and "….the cost of rework or corrective action required to remedy the use or inclusion of such parts are not allowable costs under Department contracts".[94] Therefore, the cost of ICT integrity and authenticity should already be expected and DOD contractors have a duty to conduct anti-counterfeiting due diligence.

Finally, the DOD weapon system program managers (military, government or civilian) need to be held responsible for ensuring the integrity of their weapons systems platform. The current DOD guidance presented in this research does little to provide instructions on who and what should enforce the anti-counterfeiting efforts within the Air Force. As the research has discovered the answers to these questions are buried in pages upon pages of government testimony, Federal Acquisition Regulations, DOD research and directives, all of which refer to one another without clearly delineating the responsible entity.

Recommendation 2: Reclassify Counterfeit ICT's as a Cyber Intrusion

The deliberate misrepresentation or modification of any ICT electronic component by a known adversarial nation state needs to be reclassified as a cyber-attack and not only as an economic crime. Nation states are knowingly developing counterfeit, and substandard electrical components that are directly targeting our national defense industrial base. The global supply chain threat has emerged into an intricate criminal cyber ecosystem that has developed into a multibillion-dollar business complete with a management structure, quality control and global customer base.

One of the biggest ICT security concerns affecting the Federal Government is described as the insider threat. A 2014 industry survey of 200 ICT security decision makers, working within the Federal Government, was conducted to research insider and external ICT security threats. The organizations represented federal, civilian or independent government agency (54%), DOD or military service (39%), federal judicial branch (3%), intelligence agency (3%) and federal legislature (2%) (Appendix-A). The survey results concluded that the largest source of cyber security risks at federal agencies are insider threats (53%) followed by hacking (46%), foreign governments (38%), hacktivist (30%), malicious insiders (23%) and terrorists (18%) (Appendix-B).

The insider threat is typically characterized as an employee who has authenticated to the internal enterprise network and purposively conducts malicious activities to disrupt, deny or steal information systems. However, the researcher is presenting the insider threat as an appliance or electrical component that infiltrates a weapon platform through the Federal Supply system.[95] For example, China's intelligence agencies recognize that the USAF is still maintaining mission critical legacy aircraft; they understand the budgetary constraints imposed by sequestration; they know legacy replacement parts for these aircrafts are difficult to find[96] and the economic theory associated with supply and demand costs. Leveraging this information from these factors, China now has a predefined attack vector. Using social engineering and advanced counterfeiting techniques, China is able to break into a weapon system and deliver targeted malware or a substandard electrical component. The discovery of this intrusion is very difficult using the current ICT SCRM framework because the electronic component appears and functions as an OEM product until system failure. The insider

ICT threat is a vetted electrical component within a trusted environment and surreptitiously lies dormant in a vulnerable weapon system.

An investigation by the U.S. House of Representatives on the U.S. National Security Issues by Chinese telecommunication companies Huawei and ZTE describes the groundwork for an advanced persistent threat.[97] The investigation revealed that sensitive U.S. government systems should not use ICT components from these companies due to counterintelligence and cyber espionage concerns.[98]

Using counterfeit NNSS ICT equipment purchased from China is a significant vulnerability for U.S. national security. The concern arises from counterfeit ICT routers or switches purchased from China that are plagued with security holes and backdoors enabling them for surveillance.[99] Acting as an insider threat, the compromised ICT appliance hardware creates a significant advanced persistent threat.

Recommendation 3: Senior Leadership Support

Cyber security awareness issues that resonate with senior military and DOD leaders typically involve discussions around supervisory control and data acquisition (SCADA) threats, malware, theft of intellectual data and cyber intrusions. Cyber security concerns related to counterfeit electronics are not considered high priority and are often left out of leadership top security issues. Navy Adm. Michael S. Rogers, the Commander for the United States Cyber Command (CYBERCOM), provided an executive overview on the main cyber threats facing the U.S. Although he described the above-mentioned cyber threats, Adm. Rogers did not identify any cyber security concerns related to counterfeit electronics found in advanced weapon systems.

To mitigate the high-risk level associated with counterfeit electronics, leaders

need to understand the threat capability. Additionally, the anti-counterfeiting budget needs to recognize this persistent threat by providing adequate funding for the research and development of new and innovated ways to identify and discern substandard electrical components.

Recommendation 4: Proactive Network Defense: Preventing ICT Counterfeiting

The ability to develop techniques that provide security mangers with actionable intelligence to predict human behavior has gained considerable interest. Predictive analytics uses empirical data (public or private) to try and determine future cyber-crime actions. Law enforcement officials are currently using predictive analytics to identify future criminal activities based on social media activity.

Criminal justice researchers have leveraged the emerging field of computational criminology, which combines the advances in computer technology and crime statistics, to help predict future crime in geographical areas. This same approach can be used to develop innovative methodologies to understand the AF counterfeiting cyber-crime phenomena and aid in the geographical targeting of anti-counterfeiting efforts. The capability to simulate the probability of counterfeiting techniques and patterns highlights the benefits of the computation criminology field. By studying the conditions that influence counterfeiting activities, such as electronic E-waste, anti-counterfeiting efforts can target specific electronic components and simulate potential supply chain security risks.

Applying predictive analytics and computational criminology to the AF supply chain counterfeiting problem, researchers can model an adversary's behavior by studying temporal events and using these incidents to identify certain indicators or trade crafts to

simulate areas of interest and propose anti-counterfeiting strategies. For example, let's assume the triggering event is categorized as 300,000 semiconductor components (E-waste) are sold to China. Using predictability assessments and computational criminology simulations on the known purchaser, we can identify past criminal behavior that can be studied to ascertain the counterfeit attack strategy; the adaptive behavior of the counterfeiter to previous anti-counterfeiting enforcement strategies; and also understand the current criminal counterfeiting patterns used in that geographical region.

CONCLUSION

The information presented throughout this research highlights the significance of electronic counterfeiting security risks; the historical implications of poor anti-counterfeiting strategies; and the lack of overall counterfeiting cyber security awareness. The risk of counterfeit electronics existing in AF weapons systems is a significant securities concern for military leaders and more importantly our Airmen who we call on to achieve political and strategic objectives around the globe.

The AF supply chain risk management approach is a policy driven methodology for conducting risk management and identifying associated mitigation costs. Military budget sequestration has created a significant impact on weapon system platforms and more often the risk versus cost trade off occurs. However, the cost of not funding appropriate risk mitigation strategies implies we are accepting the risk and transferring the possibility of weapon system failure to our Airmen. This is an irresponsible approach towards managing men and women in uniform as well as the development of advanced weapon platforms. We owe this cost burden to our Airmen and AF leaders must ensure adequate funding is provided to guarantee anti-counterfeiting techniques are factored into

all AF weapon system development and maintenance (to include replacement parts). This cyber security threat will require additional appropriation funding in the future to adequately support the development of sophisticated anti-counterfeiting strategies; targeted intelligence operations; and ensuring contractors are conducting due diligence in preventing electronics counterfeit products from entering the federal supply chains.

The military systems ensure our national security and protect the military men and women in uniform who are dependent on the performance and reliability of incredibly sophisticated technology components. Fighter pilots and Special Forces conducting coordinated operations rely on night vision systems, air-to-ground radios and laser-guided bombs, all of which are enabled by semiconductors and microprocessors that are incredibly small. Military men and women rely on the performance and dependability of highly sophisticated technology to preserve a technological advantage on the battlefield against our adversaries.[100] Consequently, the failure of any electrical component or semiconductors can leave a soldier, Airman, sailor, or Marine vulnerable to defeat.[101]

APPENDIX A

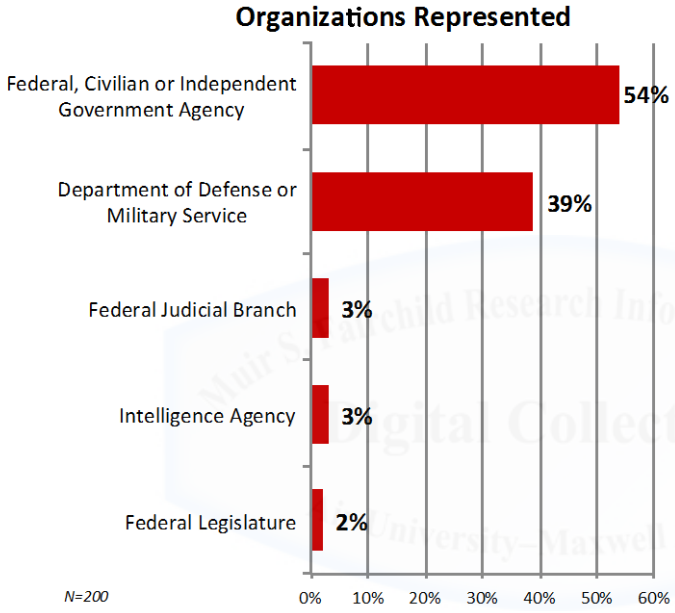
Demographics on Federal Cyber Security Survey

RESPONDENT CLASSIFICATIONS 3

Organizations Represented

solarwinds

- If a respondent did not work for any of the specific organization types noted below, the survey was terminated.

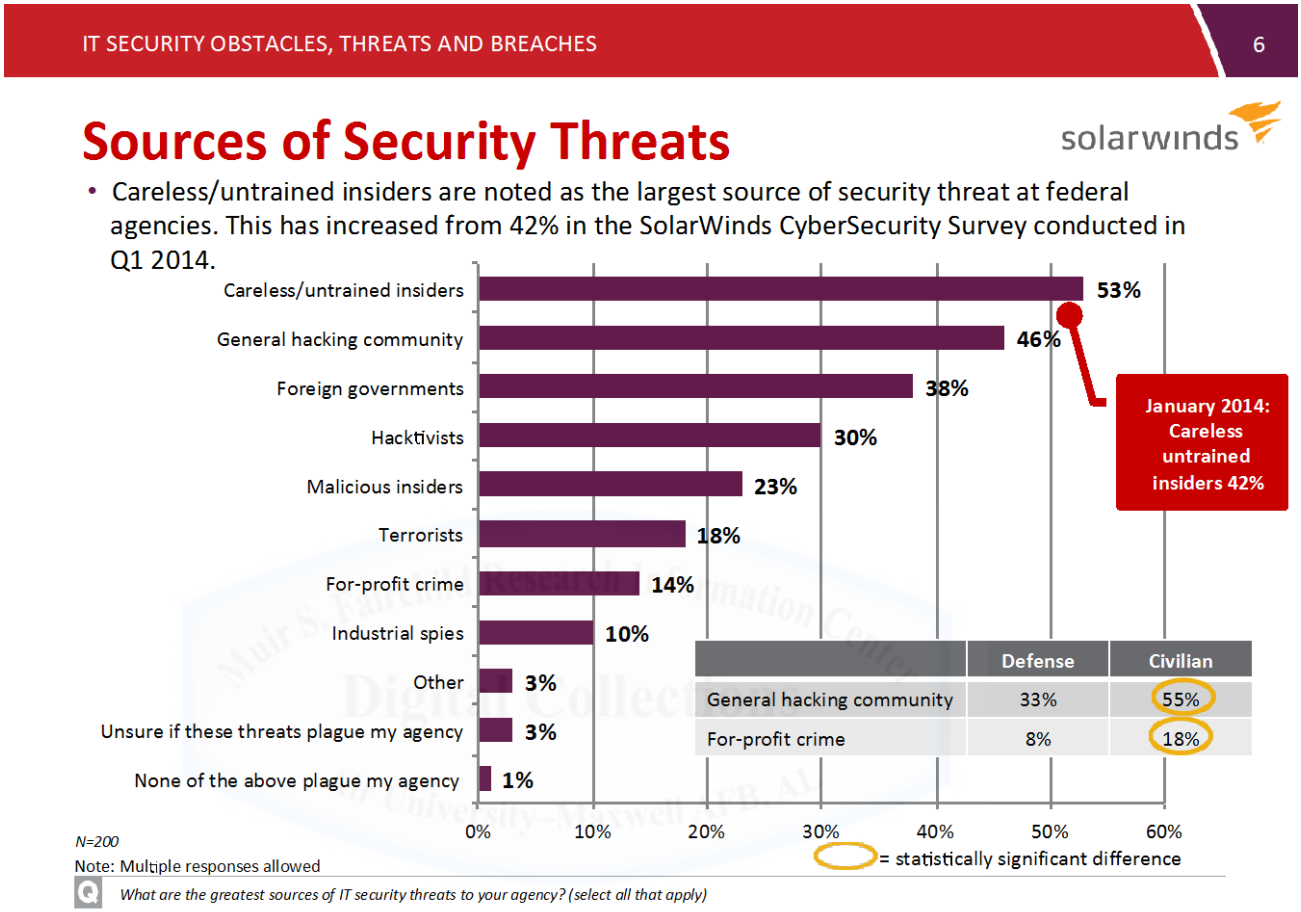


Sample Organizations Represented (In Alphabetical Order)	
Air Force	Department of the Interior (DOI)
Army	Department of Transportation (DOT)
Department of Agriculture (USDA)	Department of Treasury (TREAS)
Department of Commerce (DOC)	Department of Veteran Affairs (VA)
Department of Defense (DOD)	Environmental Protection Agency (EPA)
Department of Energy (DOE)	Judicial/Courts
Department of Health and Human Services (HHS)	Marine Corps
Department of Homeland Security (DHS)	National Aeronautics and Space Administration (NASA)
Department of Labor (DOL)	Navy
Department of Justice (DOJ)	Social Security Administration (SSA)
Department of State (DOS)	US Postal Service (USPS)

Q *Which of the following best describes your current employer? What agency do you work for?*

APPENDIX B

Survey results identifying cyber threat sources.



BIBLIOGRAPHY

"Addressing Counterfeit Semiconductor Products." World Semiconductor Council Anti-counterfeiting Task Force.

"AFOSR: Information and Networks." *The Air Force Research Laboratory*, 2015. http://www.wpafb.af.mil/library/factsheets/factsheet.asp?id=9204.

Arthur, Charles. "China's Huawei and ZTE Pose National Security Threat, Says US Committee." The Guardian. October 8, 2012. http://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat.

Bodner, Douglas A. "Enterprise Modeling Framework for Counterfeit Parts in Defense Systems." *Procedia Computer Science* 36 (2014): 425-31. doi:10.1016/j.procs.2014.09.016.

Bodner, Douglas A. "Enterprise Modeling Framework for Counterfeit Parts in Defense Systems." *Procedia Computer Science* 36 (2014): 425-31. doi:10.1016/j.procs.2014.09.016.

Boyens, Jon M., Celia Paulsen, Rama Moorthy, and Nadya Bartol. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations." 2015. doi:10.6028/nist.sp.800-161.

Burger, Jim, Henry Livingston, and Tom Sharpe. "Electronic Waste Rules Could Help Thwart Flow of Counterfeit Parts." *National Defense*, February 2015. http://www.nationaldefensemagazine.org/archive/2015/February/Pages/ElectronicWasteRulesCouldHelpThwartFlowofCounterfeitParts.aspx.

Caims, Lisa. "Counterfeit Mitigation: Solutions, Not Scapegoats." August 2015. Electronic Purchasing Strategies.

Caims, Lisa. "NDAA Raises Stakes on Component Traceability." September 2015. Electronic Purchasing Strategies.

Caims, Lisa. "Proposal Would Tighten DFARS Sourcing Rule." September 2015. Electronic Purchasing Strategies.

Caims, Lisa. "Sourcing Strategies and the "Trusted Supplier" Conundrum." September 2015. Electronic Purchasing Strategies.

The Committees Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain, 112th Cong., 2 (2011) (testimony of Senator Carl Levin).

Cooney, Michael. "DARPA Partners Are Developing Technologies and Software That Can Certify Circuits." October 2014. NETWORKWORLD.

Creswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage, 2009.

Cribbin, Timothy. "Citation Chain Aggregation: An Interaction Model to Support Citation Cycling." Proceedings of Proceedings of the 20th ACM Conference on Information and Knowledge Management, Glasgow, UK. October 28, 2011.

(Csd), Nist Computer Security Division. *NISTIR 7622 Draft, Piloting Supply Chain Risk Management Practices for Federal Information Systems (DRAFT)*, June 2010, 1-78.

Davidson, Don, and Stephanie Shankles. "We Cannot Blindly Reap the Benefits of a Globalized ICT Supply Chain!" *CrossTalk*, March 2013, 4-7.

Defense Supply Base: DoD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts. Report no. GAO-10-389. Washington, D.C. (P.O. Box 37050, Washington, D.C. 20013): Unites States Government Accountability Office, 2010.

Definitions, § 44-3532.

Doyle, Tom. "Enabling Trusted Trade through Secure Track and Trace Technology." *World Class Journal* 8, no. 1, 147-54.

"Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." *PsycEXTRA Dataset*, 2011. doi:10.1037/e741782011-001.

The Federal Bureau of Investigations. "Chinese Businessman Charged with Theft of Trade Secrets." News release, October 2015. The Federal Bureau of Investigations.

The Federal Bureau of Investigations. "Former PPG Employee Charged with Theft of Trade Secrets." News release, May 2015. The Federal Bureau of Investigations.

Federal Bureau of Investigations. "Two Miami-Based Aircraft Parts Suppliers Plead Guilty in Procurement Fraud Scheme." News release, April 2010. The Federal Bureau of Investigations.

Filsinger, Jarrellann, Barbara Fast, Daniel G. Wolf, James F.X. Payne, and Mary Anderson. "Supply Chain Risk Management Awareness." *ARMED FORCES COMMUNICATION AND ELECTRONICS ASSOCIATION CYBER COMMITTEE*, February 2012, 1-13.

Francq, Julien, and Florian Frick. "Introduction to Hardware Trojan Detection Methods." *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*, 2015. doi:10.7873/date.2015.1101.

Gebicke, Scott. "EMS Provider Combat Electronics Counterfeiting with Supply Chain Controls." September 2013. Military Aerospace.

Gerstein, Daniel M. *Strategies for Defending U.S. Government Networks in Cyberspace*. Report. RAND, 2015.

Gittlen, Sandra. "Technology That Predicts Your next Security Fail." Computerworld. Accessed December 10, 2015. http://www.computerworld.com/article/2982306/security/technology-that-predicts-your-next-security-fail.html.

Glick, Bryan. "Dont Buy from IT Suppliers with a Poor Track Record." COMPUTERWEEKLY.COM. October 2013. Computer Weekly.

Gottlieb, Craig. "Investing in a Secure High Tech Supply Chain: Technology Supply Chains Are Extremely Vulnerable--and as Craig Gottlieb, Senior Manager in Accenture's Supply Chain Management Practice, Suggests, Not Only in Areas That Consumers Would Regard as 'hi Tech.'." *Supply Chain Europe*, January 1, 2011.

Houghton, Peter. "Potential System Vulnerabilities of a Network Enabled Force." *Defense Scientific and Technical Labratory*, 2004, 1-27.

Hsu, D. Frank, Dorothy Marinucci, and Jeffrey M. Voas. "Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem." *Computer* 48, no. 4 (2015): 12-14. doi:10.1109/mc.2015.103.

"Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems." United States Government Accountability Office. September 2010. Accessed December 08, 2015. http://www.gao.gov/products/GAO-10-916.

"Insider Threat." Insider Threat. 2015. Accessed December 08, 2015. http://www.cert.org/insider-threat/.

Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC Press, 2011.

Justice Department. Naval Criminal Investigative Service. "Massachusetts Man Charged with Selling Counterfeit Semiconductors Intended for Use on Nuclear Submarines." News release, July 2013. Unites States Department of Justice.

Kae-Nune, Nathalie, and Stephanie Pesseguier. "Qualification and Testing Process to Implement Anti-Counterfeiting Technologies into IC Packages." *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, 2013. doi:10.7873/date.2013.237.

Karisny, Larry. "Cybersecurity: Taking a Proactive Approach Is Key." *GOVERNING*, March 4, 2015. www.governing.com.

Keller, John. "Draper Lab Takes Aim at Military Counterfeit Electronics in Work on DARPA SHIELD Program." January 2015. Military Aerospace.

Koushanfar, Farinaz, Saverio Fazzari, Carl Mccants, William Bryson, Matthew Sale, Peilin Song, and Miodrag Potkonjak. "Can EDA Combat the Rise of Electronic Counterfeiting?" *Proceedings of the 49th Annual Design Automation Conference on - DAC '12*, 2012, 133-38. doi:10.1145/2228360.2228386.

Lamb, Robert L., Christopher Ling, and Randy Hayes. *Building Enterprise-wide Cybersecurity That Learns, Adapts, and Proactively Combats Rapidly Changing Cyber Threats.* Technical paper. 2012.

Livingston, Henry. *Compliance Programs for Counterfeit Parts Avoidance and Detection*. Technical paper. Accessed March 4, 2013.

Lowry, Robert K. *Oneida Research Services.* Technical paper. 2015. https://www.ors-labs.com/pdf/MASH07CounterfeitDevice.pdf.

McHale, John. "Threat of Counterfeit Parts to Defense Supply Chain Getting Worse." *Military Embedded Systems*.

Moore, Jack. "Why Federal CIO Tony Scott Hate The End of Year IT Spending Spree." Newsgroup. August 27, 2015. Nextgov.

Mwikali, Ruth, and Stanley Kavale. "Factors Affecting the Selection of Optimal Suppliers in Procurement Management." *International Journal of Humanities and Social Science* 2, no. 14 (July 2014): 189-93.

Netmarcom, Symantec. "Advanced Persistent Threats: A Symantec Perspective." *Symantec White Paper - Advanced Persistent Threats: A Symantec Perspective*: 1-7. http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

Pecht, Michael. "The Counterfeit Electronics Problem." *JSS Open Journal of Social Sciences* 01, no. 07 (2013): 12-16. doi:10.4236/jss.2013.17003.

Pettit, Timothy J., Joseph Fiksel, and Keely L. Croxton. "Ensuring Supply Chain Resilience: Development Of A Conceptual Framework." *Journal of Business Logistics* 31, no. 1 (2010): 1-21. doi:10.1002/j.2158-1592.2010.tb00125.x.

Ravindranath, Mohana. "DOD's Current Infosec Strategy Is "Patch and Pray"" Newsgroup. October 1, 2015. Defense One.

Rostami, Masoud, Farinaz Koushanfar, and Ramesh Karri. "A Primer on Hardware Security: Models, Methods, and Metrics." *Proceedings of the IEEE Proc. IEEE* 102, no. 8 (2014): 1283-295. doi:10.1109/jproc.2014.2335155.

Rouse, Margaret. "What Is ICT (information and Communications Technology - or Technologies)? - Definition from WhatIs.com." SearchCIO. September 2005. Accessed December 08, 2015. http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies.

Rouse, Margaret. "What Is OEM (original Equipment Manufacturer)? - Definition from WhatIs.com." SearchITChannel. April 2015. Accessed December 08, 2015. http://searchitchannel.techtarget.com/definition/OEM.

S. Rep. No. 112-112-167 at 3 (2012).

Szakal, A. R., and K. J. Pearsall. "Open Industry Standards for Mitigating Risks to Global Supply Chains." *IBM Journal of Research and Development IBM J. Res. & Dev.* 58, no. 1 (2014). doi:10.1147/jrd.2013.2285605.

Taylor, Phil. "DARPA Unveils First Images of Chip 'dielet'" *Securing Industry*, September 2015.

"Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market." *IHS*, April 4, 2012. http://press.ihs.com/press-release/design-supply-chain/top-5-most-counterfeited-parts-represent-169-billion-potential-cha.

United States. Executive Office of the President of the United States. The United States Trade Represenative. *The Office of the Unites States Trades Represenative.* By Michael B.G. Froman. April 2015. https://ustr.gov/sites/default/files/2015-Special-301-Report-FINAL.pdf.

United States. General Accounting Office. *Best Practices Better Management of*

Technology Development Can Improve Weapon System Outcomes: Report to the Chairman and Ranking Minority Member, Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate. Washington, D.C. (P.O. Box 37050, Washington, D.C. 20013): Office, 1999.

United States. Homeland Defense. Executive Office of the President of the United States. *The Comprehensive National Cybersecurity Initiative.* 2008. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

United States. Office of the National Counterintelligence Executive. *ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace.* October 2011. Accessed November 23, 2015. http://www.dni.gov/index.php/newsroom/reports-and-publications/94-reports-publications-2011/616-oncix-foreign-spies-stealing-us-economic-secrets-in-cyberspace.

USA. Air Force. Audit Agency. *Information Technology Asset Management*. F2015-0002-O10000.

USA. Department of Defense. *DoD Counterfeit Prevention Policy*. Series 4140.67. 2013.

USA. Executive Office of the President of the United States. Office of the United States Trade Represenative. *Results of the 2014 Out-of-cycle Review of Notorious Markets*. Washington: USTR, 2015. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2015/2014-notorious-markets-list.

USA. National Institute of Standards and Technology. U.S. Department of Commerce. *Information Security*. 800-30. Washington: Department of Commerce, 2012.

"U.S.-CHINA." U.S.-CHINA. Accessed December 06, 2015. http://www.uscc.gov/.

Vakil, Bindiya, and Hanna Kain. *The Top 5 Mistakes Companies Make in Managing Supply Chain Risk Effectively*. Technical paper. RESIL.

"White Hat Hacker Definition from PC Magazine Encyclopedia." White Hat Hacker Definition from PC Magazine Encyclopedia. 2015. Accessed December 08, 2015. http://www.pcmag.com/encyclopedia/term/54434/white-hat-hacker.

Wilkerson, Taylor. "Cyber Security in the Supply Chain." Newsgroup. 2014. United States Cybersecurity Magazine.

"Winning the Battle Against Counterfeit Semiconductors Products." *Semiconductor Industry Association*, 2013. http://www.semiconductors.org/clientuploads/Anti-Counterfeiting/SIA%20Anti-Counterfeiting%20Whitepaper.pdf.

Notes

---

1. Netmarcom, Symantec. "Advanced Persistent Threats: A Symantec Perspective." *Symantec White Paper - Advanced Persistent Threats: A Symantec Perspective*:, 1.

2. Lowry, Robert K. *Oneida Research Services.* Technical paper. 2015, para.1

3. Inquiry into counterfeit electronics parts in the Department of Defense supply chain, Committee on Armed Services United States Senate, (S. rep. No. 112th-112-167 at I) (May 21,2012), i.

4. Burger, Jim, Henry Livingston, and Tom Sharpe. "Electronic Waste Rules Could Help Thwart Flow of Counterfeit Parts." *National Defense*, February 2015, 1

5. Rouse, Margaret. "What Is ICT (information and Communications Technology - or Technologies)? - Definition from WhatIs.com." SearchCIO. September 2005. Accessed December 08, 2015, para. 1.

6. "Insider Threat." Insider Threat. 2015. Accessed December 08, 2015, 1.

7. Definitions, § 44-3532.

8. "Information Security: Progress Made on Harmonizing Policies and Guidance for National Security and Non-National Security Systems." United States Government Accountability Office. September 2010, 2.

9. Rouse, Margaret. "What Is OEM (original Equipment Manufacturer)? - Definition from WhatIs.com." SearchITChannel. April 2015, 1.

10. USA. National Institute of Standards and Technology. U.S. Department of Commerce. *Information Security*. 800-30. Washington: Department of Commerce, 2012.

11. "White Hat Hacker Definition from PC Magazine Encyclopedia." White Hat

Hacker Definition from PC Magazine Encyclopedia. 2015, .

12. Ibid., 3.

13. Ibid., i.

14. Pecht, Michael. "The Counterfeit Electronics Problem." *JSS Open Journal of Social Sciences* 01, no. 07 (2013): 12-16.

15. Ibid., 13.

16. Vakil, Bindiya, and Hanna Kain. *The Top 5 Mistakes Companies Make in Managing Supply Chain Risk Effectively*. Technical paper. RESIL.

17. Ravindranath, Mohana. "DOD's Current Infosec Strategy Is "Patch and Pray"" Newsgroup. October 1, 2015. Defense One.

18. Bodner, Douglas A. "Enterprise Modeling Framework for Counterfeit Parts in Defense Systems." *Procedia Computer Science* 36 (2014): 425-31.

19. Lamb, Robert L., Christopher Ling, and Randy Hayes. *Building Enterprise-wide Cybersecurity That Learns, Adapts, and Proactively Combats Rapidly Changing Cyber Threats.* Technical paper. 2012.

20. Filsinger, Jarrellann, Barbara Fast, Daniel G. Wolf, James F.X. Payne, and Mary Anderson. "Supply Chain Risk Management Awareness." *ARMED FORCES COMMUNICATION AND ELECTRONICS ASSOCIATION CYBER COMMITTEE*, February 2012, 1-13.

21. Szakal, A. R., and K. J. Pearsall. "Open Industry Standards for Mitigating Risks to Global Supply Chains." *IBM Journal of Research and Development IBM J. Res. & Dev.* 58, no. 1 (2014), 1.

22. International Chamber of Commerce, *Counterfeiting Intelligence Bureau*, 2015, para. 4.

23. Ibid.

24. Marianne Swanson, Nadya Bartol, Rama Moorthy, “Piloting Supply Change Risk Management Practices for Federal Information Systems”, National Institute of Standards and Technology (NIST), (U.S. Department of Commerce), 2010, 1.

25. S. rep. No. 112th-112-167 at I, ii.

26. Ibid., ii.

27. Ibid., iii.

28. Cribbin, Timothy. "Citation Chain Aggregation: An Interaction Model to Support Citation Cycling." Proceedings of Proceedings of the 20th ACM Conference on Information and Knowledge Management, Glasgow, UK. October 28, 2011.

29. Ibid., 1.

30. Creswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage, 2009, 10.

31. Computer Security Act of 1987 .

32. Ibid., 9.

33. Ibid., 10.

34. Ibid., 7.

35. Ibid., 17.

36. Ibid.

37. DOCID: 4123697; White House Memorandum for Recipients of NSPD-54/HSPD-23; Declassified 6-5-2014, FOIA Case#58987.

38. *The Comprehensive National Cybersecurity Initiative.* 2008,1.

39. Ibid., 5.

40. Ibid., 5.

41. Section 818, Public Law 112-81, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011.

42. Department of Defense Instructions 4140.67, "DOD Counterfeit Prevention Policy", April 26, 2013.

43. United States. Office of the National Counterintelligence Executive. ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace. October 2011, i.

44. Ibid., iv

45. Szakal et al., "Open Industry Standards for Mitigating Risks to Global Supply Chains.",

46. A. Smith, Citi: Millions Stolen in May Hack Attack, Jun. 27,2011.

47. S. rep. No. 112th-112-167 at I, iv

48. DoD Comptroller. Rep. No. 1 - A2BB24 at 107 (2015).
49. S. rep. No. 112th-112-167 at I, iv.

50. Ibid., 54.

51. "Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes: NSIAD-99-162." *GAO Reports*, July 30, 1999, 1.

52. "Winning the Battle Against Counterfeit Semiconductors Products." *Semiconductor Industry Association*, 2013, 1.

53. Moore, Nancy Y., and Elvira N. Loredo. "Identifying and Managing Air Force Sustainment Supply Chain Risks." Identifying and Managing Air Force Sustainment Supply Chain Risks. 2013,.

54. *The Committees Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 112th Cong., 2 (2011) (testimony of Senator Carl Levin).

55. Ibid.

56. "Top 5 Most Counterfeited Parts Represent a $169 Billion Potential Challenge for Global Semiconductor Market." *IHS*, April 4, 2012, para. 1.

57, Pecht,"The Counterfeit Electronics Problem.", 11.

58. Ibid., 12.

59. *The Committees Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 112th Cong., 2 (2011) (testimony of Senator Carl Levin).

60. "Winning the Battle Against Counterfeit Semiconductors Products." *Semiconductor Industry Association*, 2013,1.

61. *The Comprehensive National Cybersecurity Initiative.* 2008, Initiative 11 .

62. Ibid.

63. Jim Garamone, “Cybercom Chief Details Cyberspace Defense,” DoD News, September 23, 2010.

64. *Strategies for Defending U.S. Government Networks in Cyberspace*, Before the Committee on Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies House of Representatives Cong., 3 (2015) (testimony of Daniel M. Gerstein).

65. Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," press release, Barcelona, Spain, November 11, 2014, para.1.

66. S. rep. No. 112th-112-167 at I, vi.

67. *The Committees Investigation Into Counterfeit Electronic Parts in the Department of Defense Supply Chain*, 112th Cong., 2 (2011) (testimony of Senator Carl Levin), 3

68. "Winning the Battle Against Counterfeit Semiconductors Products." *Semiconductor Industry Association*, 2013,1.

69. United States. Cong. U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. 112 Cong., 1st sess. Cong. Rept. Washington: U.S. Government Printing Office, 2011, 8.

70. United States. ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace,1

71. United States. General Accounting Office. *Best Practices Better Management of Technology Development Can Improve Weapon System Outcomes: Report to the Chairman and Ranking Minority Member, Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate*. Washington, D.C. (P.O. Box 37050, Washington, D.C. 20013): Office, 1999

72. United States. ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace, 11.

73. Protecting you intellectual property rights in China, 2012,

74. *Results of the 2014 Out-of-cycle Review of Notorious Markets*. Washington: USTR, 2015, 9.

75. Supply Chain Risk Management Practices for Federal Information Systems and Organizations, National Institute of Standards and Technology, April 2015, 1

76. United States. ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace. October 2011,

77. Hearing Before the Committee on Armed Services United States Senate, November 8, 2011, 2.

78. *Results of the 2014 Out-of-cycle Review of Notorious Markets*. Washington: USTR, 2014. https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2015/2014-notorious-markets-list.

79. United States, Executive Office of the President of the United States, The Office of the Unites States Trades Representative, By Ambassador Michael B.G. Froman, April 2015, 1.

80. Ibid.

81. Ibid., 31.

82. 112th Cong. Testimony of Senator Carl Levin, 6.

83. Ambassador Michael B.G. Froman, April 2015, 13.

84. *Results of the 2014 Out-of-cycle Review of Notorious Markets*, 19

85. 112th Cong., Testimony of Senator Carl Levin

86. By Ambassador Michael B.G. Froman, 40.

87. United States. ONCIX: Foreign Spies Stealing US Economic Secrets in Cyberspace. October 2011. Accessed November 23, 2015.

88. By Ambassador Michael B.G. Froman, April 2015, 54

89. Unites States Senate Armed Services Committee, Confirmation Hearing, July 21, 2011.

90. Gittlen, Sandra, "Technology that predicts your next security fail", Computerworld, Sept 2015, 2

91. Ibid., 3

92. Air Force Office of Scientific Research, Information and Network Team within the Engineering and Information Science Branch, 2015, para. 1

93. National Institute of Standards and Technology (NIST) 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, U.S. Department of Commerce, April 2015, 9

94. Section 818, Public Law 112-81, "National Defense Authorization Act for Fiscal Year 2012," December 31, 2011

95. United State Government Accountability Office (GAO), DOD Supply Chain:

Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms, 2011, 1

96. Inquiry into counterfeit electronics parts in the Department of Defense supply chain, Committee on Armed Services United States Senate, (S. rep. No. 112th-112-167 at I) (May 21,2012), 88

97. United States. Cong. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE a Report. By Mike Rogers and C. A. Dutch. Ruppersberger. Cong. Bill. Washington, DC: U.S. House of Representatives, 2012,1

98. Ibid., vi.

99. Zetter, Kim. "How a Chinese Tech Firm Became the NSA's Surveillance Nightmare.". Conde Nast Digital, 27 Mar. 2014, para. 4

100. Ibid., S. rep. No. 112th-112-167, i

101. Ibid.