NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PURPOSEFULLY MANUFACTURED VULNERABILITIES IN U.S. GOVERNMENT TECHNOLOGY MICROCHIPS: RISKS AND HOMELAND SECURITY IMPLICATIONS

by

George Perera

December 2012

Thesis Advisor: John Rollins
Second Reader: Dorothy Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE PURPOSEFULLY MANUFACTURED VULNERABILITIES IN U.S. GOVERNMENT TECHNOLOGY MICROCHIPS: RISKS AND HOMELAND SECURITY IMPLICATIONS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) George Perera			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Government at all levels, industry, military and critical infrastructure, may be at risk due to purposeful manipulation of micro-processing chips during the manufacturing process. Many microchips intentionally provide remote access to allow for monitoring and updating firmware. However, a remote access capability also introduces a vulnerability, which allows others to potentially take control of a system and shut it down remotely, spy, or remove data. If this is in fact occurring, the implications to the national and homeland security could be significant. It does not appear that there are currently policies and processes to identify purposefully manufactured vulnerable micro processing chips. Should it be determined that vulnerabilities do in fact exist, a federal government-led effort is needed to identify the entities producing these chips; to assess possible intentions of these actors; inventory hardware that is in use, which may have been compromised; and, finally, to pursue the development of a remediation strategy. Additionally, the current supply chain process will have to be re-examined to mitigate current and future concerns. Therefore, in 2012, the Government Accounting Office recommended that the Department of Homeland Security (DHS) create and implement a cyber security supply chain vulnerability policy. This policy will assist the federal, state, and local governments, as well as private sector entities, to develop guidelines for procurement and policy decisions.

14. SUBJECT TERMS cyber, cybersecurity, hardware, hardware security, microchip security, supply chain security, hardware vulnerability, back door, Miami-Dade Police Department			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PURPOSEFULLY MANUFACTURED VULNERABILITIES IN U.S. GOVERNMENT TECHNOLOGY MICROCHIPS: RISKS AND HOMELAND SECURITY IMPLICATIONS

George Perera
Captain, Miami-Dade Police Department
BS, Florida International University, 1997
MS, Lynn University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2012**

Author: George Perera

Approved by: John Rollins
Thesis Advisor

Dorothy Denning
Second Reader

Harold A. Trinkunas
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Government at all levels, industry, military and critical infrastructure, may be at risk due to purposeful manipulation of micro-processing chips during the manufacturing process. Many microchips intentionally provide remote access to allow for monitoring and updating firmware. However, a remote access capability also introduces a vulnerability, which allows others to potentially take control of a system and shut it down remotely, spy, or remove data. If this is in fact occurring, the implications to the national and homeland security could be significant. It does not appear that there are currently policies and processes to identify purposefully manufactured vulnerable micro processing chips. Should it be determined that vulnerabilities do in fact exist, a federal government-led effort is needed to identify the entities producing these chips; to assess possible intentions of these actors; inventory hardware that is in use, which may have been compromised; and, finally, to pursue the development of a remediation strategy. Additionally, the current supply chain process will have to be re-examined to mitigate current and future concerns. Therefore, in 2012, the Government Accounting Office recommended that the Department of Homeland Security (DHS) create and implement a cyber security supply chain vulnerability policy. This policy will assist the federal, state, and local governments, as well as private sector entities, to develop guidelines for procurement and policy decisions.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BIOS	Basic Input/Output System
COTS	Commercial Off the Shelf Products
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DoD	Department of Defense
DSB	Defense Science Board
FBI	Federal Bureau of Investigation
FPGA	Field-Programmable Gate Array
GAO	Government Accounting Office
IARPA	Intelligence Advanced Research Projects Activity
IATAC	Information Assurance Technology Analysis Center
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NCSC	National Cyber security Center
NCIJTF	National Cyber Investigative Joint Task Force
NPS	Naval Post Graduate School
NSA	National Security Agency
OTS	Off-the Shelf
PLA	People's Liberation Army
SOAR	State of the Art Report
SCRM	Supply Chain Risk Management
TI	Texas Instruments
TSMC	Taiwan Semiconductor Manufacturing Corporation
UMC	United Microelectronics Corporation
US	United States
US-Cert	U.S. Computer Emergency Readiness Team
U.S. CYBERCOM	U.S. Cyber Command
USSS	United States Secret Service

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to express thanks to the faculty and staff at the Naval Postgraduate School (NPS), Center of Homeland Defense and Security for affording me the opportunity to participate in the program and providing me with an invaluable set of tools that I am already using and will continue to use in the future.

I would like to thank my wife, Diane, and son, Alex, for your understanding and unwavering support, through many long hours of work at school and at home.

I would like to extend special thanks to John Rollins, Dorothy Denning, and Richard Bergin who have influenced, guided and assisted me during the development of this thesis. Your help and friendship has provided me with a unique experience and a great time at NPS. Thank you for your patience and constructive critique.

Finally I wish to thank my good friend, Carlos Vazquez, for the support and cover at work. You helped me pursue this program, provided feedback on assignments, and words of encouragement when needed. I will not forget, my friend.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> *Pwned: verb, to compromise or control, specifically another computer (server or PC), Website, gateway device, or application.*[1]

Have the federal government, Department of Defense (DoD), state and local governments, and private industry and critical infrastructure all been pwned? That possibility and the potential implications will be examined in this thesis. The federal government is the largest single purchaser of technology in the world, spending more than $400 billion each year.[2] The Office of Federal Procurement policy mission is: To ensure that it spends money wisely and eliminates waste and abuse of taxpayer dollars;[3] this includes ensuring the purchase of secure and reliable equipment. Specifically, the DoD spent $33 billion on information technology during FY2012.[4] Purchases ranged from simple desktop computers to highly classified telecommunications systems.[5] Many of the hardware devices contain microchips manufactured outside of the United States.[6] In 1986, the President's Blue Ribbon Commission on Defense Management emphasized the need for Department of Defense (DoD) to expand its use of commercial off the shelf products (COTS).[7]

---

[1] "Editor," Webster's Online Dictionary, http://www.websters-online-dictionary.org/definitions/pwn (accessed October 22, 2012).

[2] Marcia G. Madsen, Louis M. Addeo, Frank J. Anderson, Jr., Dr. Allan V. Burman, Carl DeMaio, Marshall J. Doke, Jr., David A. Drabkin, Jonathan L. Etherton, James A. Hughes, Deidre A. Lee, Tom Luedtke, Joshua I. Schwartz, and Roger D. Waldron, *Report of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress* (Washington, D.C.: Congressional Budget Office, 2007).

[3] Whitehouse, *Whitehouse, Office of Management and Budget, Office of Federal Procurement*, http://www.whitehouse.gov/omb/procurement_mission (accessed October 22, 2012).

[4] Office of Management and Budget, "IT Dashboard," August 31, 2012, http://www.itdashboard.gov/portfolios (accessed October 22, 2012).

[5] Ibid.

[6] Government Accounting Office [GAO], *Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India* (Washington, DC: Government Accounting Office, 2006).

[7] President's Blue Ribbon Commission on Defense Management [The Packard Commission], *A Quest for Excellence: Final Report to the President and Appendix, Final* (Washington, D.C.: Packard Commission, 1986).

Historically, the United States (U.S.) has dominated in worldwide manufacturing and research with particular strengths in the technology sector. However, due to rising manufacturing costs and the emerging global economy, manufactures have found that they could reduce costs and increase profitability by identifying locations outside of the U.S. to move their manufacturing operations. Some of the locations with the lowest labor costs, the most expensive component of the manufacturing process, were in Southeast Asia, particularly in China.[8] As manufacturers moved their operations to these new locations, profit margins rose and a new model for the manufacturing process began.

More and more companies have continued to move their manufacturing offshore, including that for technology and computers.[9] This move was not without concern. Companies that had transferred their manufacturing process offshore were finding many of their products being counterfeited and showing up in the U.S. and the rest of the world. This became a booming industry for organizations in these countries. In particular, China's black market became the most the adept at replicating others products.[10]

With the electronics and technology sector manufacturing moving off shore, several signs began appearing, indicating that there would be a potential problem. The first sign was that consumer electronics were being counterfeited. Later, it was found that malware was being inserted into some of the electronics. One of the first examples of this situation was a digital picture frame that had malware embedded within it. When the user attached the peripheral device to their computer, the malware executed and entered their machine.[11] In July 2010, Dell preformed a recall on PowerEdge R410 Rack servers due to a malware embedded within the systems management software.[12] More recently,

---

[8] Mike Vargo, "Innovation in an Offshoring Economy," *CIT Engineering Magazine*, winter 2011.

[9] Government Accounting Office, *Offshoring*.

[10] Sharon LaFraniere, "Facing Counterfeiting Crackdown, Beijing Vendors Fight Back," *New York Times*, March 1, 2009.

[11] Gregg Keizer, "Best Buy Sold Infected Digital Picture Frames," *Computerworld Online*, January 23, 2008. http://www.computerworld.com/s/article/9058638/Best_Buy_sold_infected_digital_picture_frames (accessed October 10, 2012).

[12] John Oates, "Dell Warns on Spyware Infected Server Motherboards," *The Register Online*, July 21, 2010, http://www.theregister.co.uk/2010/07/21/dell_server_warning/ (accessed September 20, 2012).

researchers discovered malicious code developed by Chinese hackers for smart cards targeting Department of Homeland Security (DHS), DoD, and State Department personnel.[13]

Smart cards are a secondary authentication measure between passwords and the computer. After entering your password you, swipe the card to validate your identity. Once you swiped the card on an infected machine the malware in the computer steals the smartcard authentication information and pin allowing the hackers to authenticate and gain access to the networks whenever they want.[14] While there have been no confirmed unclassified reports of a compromised microchip,[15] there have been several instances of counterfeit microchips entering the supply chain. The most significant was two men from Texas who had sold the DoD, Federal Aviation Administration, Department of Energy, numerous universities and defense contractors computer equipment that was purported to be authentic when in reality was counterfeit.[16] While no official governmental reports have come out and acknowledged the issue, there have been some hints at the possibility by personnel testifying before Congress and in policy documents.[17] Some security observers are concerned that the nation is vulnerable to an emerging threat emanating from purposefully manufactured vulnerabilities in off the shelf microchips.

---

[13] Kelly Jackson Higgins, "Sykipot Malware Now Steals Smart-Card Credentials," *Information Week Online*, January 12, 2012, http://www.darkreading.com/authentication/167901072/security/attacks-breaches/232400288/sykipot-malware-now-steals-smart-card-credentials.html (accessed October 22, 2012).

[14] Ibid.

[15] For purposes of this paper, a compromised microchip is defined as integrated circuit in which security cannot be trusted.

[16] Glenn Derene and Joe Pappalardo, "Counterfeit Chips Raise Big Hacking, Terror Threats, Experts Say," *Popular Mechanics Online*, October 2009, http://www.popularmechanics.com/technology/gadgets/news/4253628 (accessed July 10, 2012).

[17] White House, *Cyber Space Policy Review* (Washington, D.C.: White House, 2009).

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW AND METHODOLOGY

A systematic literature review was conducted to assess the available information on the topic of cyber security and hardware compromise. The literature provides what is known about the topic, what is unknown, and what should be known.

Cyber attacks generally refer to criminal activity conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet, and disrupting a country's critical national infrastructure. Literature derived from government reports, peer-reviewed articles, and books establish the basis of the review of cyber security.

Of particular interest is hardware compromise. There has been much speculation about the potential of the microchip supply chain being vulnerable to manipulation. This can occur via counterfeit products or with the actual fabrication of microchip that contains a built in backdoor or kill switch. Have the security implications of hardware been considered? If the actual hardware infrastructure that the services ride on is compromised then all processes that follow, no matter what precautions are taken, will be at risk as well.

The literature review involved three main steps. The first step was to identify keywords for use in the on-line search process (Table 1). The search topics were intentionally broad to capture a variety of information on this topic. Secondly, a systematic review of search engines (Google, Google Scholar) and graduate school on-line libraries (Dudley Knox) was performed on the key word list. After relevant sources were identified, they were reviewed to determine if they addressed the topic sufficiently.

Table 1. Keywords Used in Guiding the Systematic Literature Review

Keyword List		
Generic	Hardware compromise; Cyber security; Microchip compromise; Counterfeit microchip; Microchip backdoor	
Sector	Government	Private Sector
Specific	Vulnerabilities; Microchip; Cyber; Cyber Security; Microchip compromise; Counterfeit microchip; Microchip backdoor	Vulnerabilities; Microchip; Cyber; Cyber Security; Microchip compromise; Counterfeit microchip; Microchip backdoor

Current information was sought from January 2009 forward from a variety of sources including: government and non-government information, journals, books, media, databases, and online articles. In addition, both peer reviewed and non-peer reviewed literature were considered. This review was intended to identify resources that would aid in understanding microchip fabrication, cyber security, counterfeit microchips, and how microchips can introduce vulnerabilities in homeland security.

More than 20 sources have been identified. Some have been analyzed for their relevance to the study of cloud computer hardware compromise and cyber security; this is an ongoing process. Sources that addressed cyber security in general, but did not specifically address the hardware or microchips, were considered for their application to the broader topic. For example, it is important to understand the methods of cyber security before looking deeper into hardware vulnerabilities.

The literature review revealed a significant amount of information on the hypothetical possibility of a manufactured vulnerability but not much in documented cases. These sources included government databases, peer reviewed journal articles, books written by experts, and articles from those studying terrorism inside and outside of government.

A. HARDWARE VULNERABILITIES

The first consideration is whether computer hardware, more specifically, whether microchips are vulnerable to being hacked or compromised during manufacture. In order to address this, a comprehensive examination of the process would have to be conducted. Key to this would be the design process as well as the manufacturing process. The security and quality control validation at both points, with an emphasis on the facilities, is critical.

Of specific concern would be the quality of hardware being used, specifically, whether it was an original or a counterfeit. There have been numerous instances of the sale of counterfeit computer microchips to the Department of Defense.[18] This has the potential for corrupting many critical systems. Also in the same DoD report, supply concerns are of significance because "it opens the possibility that Trojan Horses and other unauthorized design inclusions may appear…."[19]

According to Sally Adee in "The Hunt for the Kill Switch," another vulnerability that has the potential for impacting homeland security is the dependence on foreign suppliers. In this instance, all manufacturers, with the exception of one IBM plant, are outside of the United States, and the majority in South East Asia.[20] Should an issue arise within one of these countries that is a major fabricator, adverse impacts could be felt through the lack of supply. This could either be intentional, such as a political measure, or unintentional, such as an accident or act of god.

A serious concern would be the inability to share secure communications, either voice or data. The implication of this would be catastrophic if, during a conflict, the adversary had the ability to monitor any information sent via a computer system. Another would be the ability to shut down a critical system remotely. The impact of this could be enormous if flight control systems, weapons systems, or other critical infrastructure were shut down. The DoD Task Force on High Performance Microchip

---

[18] Defense Science Board, *High Performance Microchip Supply* (Washington, D.C.: Department of Defense, 2005).

[19] Ibid.

[20] Sally Adee, "The Hunt for the Kill Switch," *Spectrum, IEEE* 45, no. 5 (2008).

Supply stated, "If real and potential adversaries ability to subvert the US microelectronics components is not reversed or technically mitigated, our adversaries will gain enormous asymmetric advantages that could possibly put the US force projection at risk"[21]

There have been numerous papers written about the potential for microchip compromise and the impact it could have on various facets of government and industry. The University of Illinois Computer Science Department sought to prove that it is possible to implant an undetectable vulnerability on a microchip. They then did it and provided the compromised chip along with uncompromised chips to researchers to see if they could determine which one was the compromised chip. This was done utilizing current technology. The researchers were not successful in finding the vulnerability, so the university was able to prove their point that it can be done.[22] The concern is significant enough to warrant DARPA and IARPA to begin initiatives to identify potential microchip vulnerabilities.[23] Currently, the process of identification of compromised microchips is very difficult and time consuming, requiring destructive testing and reverse engineering. Even in doing so, the correct identification of a potential vulnerability is not a sure thing.

Only recently are governmental agencies looking seriously at the possibility of microchip vulnerability. The reason they have not thus far, according to Carl McCants, Program Manager at DARPA, is because there have been no documented instances that a microchip has been compromised.[24] He went on to say there has been speculation and instances of malware being inserted on a platform, but there are no attributions of this having occurred.[25]

---

[21] Defense Science Board, *High Performance Microchip Supply*.

[22] Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, Yuanyuan Zhou, and Samuel T. King, *Designing and Implementing Malicious Hardware* (Urbana, IL: USENIX Association, 2008).

[23] Federal Business Opportunities, "DARPA," https://www.fbo.gov/?s=opportunity&mode=form&id=406db188e0e1935a806c143a5603eb48&tab=core&_cview=0 (accessed January 28, 2012).

[24] Carl McCants (DARPA Program Manager), interview with author, February 15, 2012.

[25] Ibid.

In July 2010, Dell recalled its PowerEdge R410 Rack servers due to a malware embedded within the systems management software.[26] More recently, researchers discovered malicious code developed by Chinese hackers on smart cards targeting DHS, DoD, and State Department personnel. Smart cards are a secondary authentication measure between passwords and the computer.

According to Sergei Skorobogatov of Cambridge University, the threat does exist, in fact.[27] He has recently developed a non-invasive/non destructive testing process for microchips. Cambridge University is the first research institution that has successfully tested off the shelf DoD field programmable gate array (FPGA) chips in use today and found a preprogrammed backdoor in the hardware of the microchip itself. The implications of this finding are very significant. This raises serious questions about the integrity of the manufacturers and their respective security practices. As a result of these findings, decisions will have to be made as how to remediate what is already in production and how security is enforced in future production.[28]

B. CYBER SECURITY

Attacks on computer systems can range from disruption of critical infrastructure to financial gain, and they are relatively new for the world of criminal investigations. The definition of cybercrime is criminal activity done using computers and the Internet.[29] The scope is very broad and growing more so each day as more illegal computer activities are being done and identified.

During the month of August, there were 30 documented serious incidents of hacktivism. Hacktivism is defined as the use of computers and computer networks as a means of protest to promote political ends.[30] Some of the tools that are used include

---

[26] John Oates, "Biting the Hand that Feed IT," *The Register*, July 21, 2010.

[27] Sergei Skorobogatov and Christopher Woods, *Breakthrough Silicon Scanning Discovers Backdoor in Military Chip* (Cambridge, MA: Cambridge University, 2011).

[28] Ibid.

[29] Techterms Computer Dictionary, s.v. "cybercrimes," http://www.techterms.com/definition/cybercrime (accessed September 22, 2011).

[30] Alexandra Samuel, "Hacktivism and the Future of Political Participation," August 2004, http://www.alexandrasamuel.com/dissertation/index.html (accessed July 15, 2012).

Website defacements and redirects, denial-of-service attacks, information theft, Website parodies, and virtual sabotage, all of which are crimes that can be investigated and prosecuted.

Cyber criminals are increasingly adept at gaining undetected access to IT systems. They keep a low profile and are capable of maintaining a long-term presence in IT environments. Organizations seem to focus heavily on antivirus and blocking pornography, while potential cybercrimes may be going on undetected and unaddressed. They may be leaving themselves vulnerable to cybercrime based on a false sense of security, perhaps even complacency, driven by the use of these security tools and processes. This has created an environment of significant risk exposure, including financial losses and data breach.

According to IT professionals, the insider threat of a rogue employee is more likely to occur than an instance of hacking.[31] In the report *State of Security: What Keeps Infosec Pros Awake at Night,*[32] Wilson identifies what IT professionals consider to be the most significant threats. He goes on to cite numerous studies and statistics for the various methodologies cyber criminals and hackers use to gain access to data.[33] Wilson addresses budgetary issues that IT security management needs to be cognizant of as well as expectations of organizational management.[34] The downfall of the article was that it did not address best practices or suggest some strategies form IT security professionals to employ. The only suggestion made was to ensure that users were adequately trained in information security techniques.[35] There has been a recent trend in IT security to train end users in some basic information security techniques. Wilson advocates for education that could potentially cut down on the insider threat, which in his opinion is the most

[31] Tim Wilson, "State of Security: What Keeps Infosec Pros Awake at Night?" *Information Week,* February 2009.

[32] Ibid.

[33] Ibid.

[34] ibid

[35] Ibid.

significant issue.[36] Thereby, Wilson reduces his IT security risk exposure.[37] A more comprehensive look at best practices could identify some potential policy strategies that IT security staff could employ to reduce their risk.

C. A HOMELAND SECURITY VULNERABILITY

Another concern for homeland security is a potential attack on critical infrastructure. For the most part, an attack on critical infrastructure would most likely be related to some type of terrorist activity, but it cannot be ruled out that it could be someone testing their hacking ability with no terrorism nexus at all. Cyber terrorism is a real and emerging threat in the homeland security arena that is gaining momentum daily. There are ever increasing groups and companies that are willing to provide destructive services to the highest bidder.[38] A small country or group with limited backing could potentially purchase a cyber weapon, deploy it and cripple a target's critical infrastructure, financial system, or even military.[39]

This concern is not without grounds. For example, the Government Accounting Office (GAO) reported a dramatic increase in cyber attacks on federal agencies, as reported to the U.S. Computer Emergency Readiness Team (US-Cert). The cyber incidents totaled 41,776 in fiscal 2010, a 650 percent increase in five years.[40]

The specter of a potential attack, coupled with the increased incidents in hacking, have resulted in the creation of new policy and sections within the Department of Homeland Security (DHS) and Department of Defense (DoD), in addition to the Federal Bureau of Investigation (FBI), to prepare for, prevent, and mitigate attacks on the United States and its interests.[41]

---

[36] Wilson, "State of Security."

[37] Ibid.

[38] Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," *Bloomberg Business Week*, July 20, 2011.

[39] Ibid.

[40] Peter Behr, "A 'Smart' Grid Will Expose Utilities to Smart Computer Hackers," *New York Times*, April 19, 2011.

[41] White House, *International Strategy for Cyberspace* (Washington, D.C.: White House, 2011).

In anticipation of potential attacks against U.S. interests in 2008, DHS created the National Cyber Security Center (NCSC). The NCSC is tasked with protecting the government's cyber networks and will monitor, collect, and share information regarding cyber security incidents on systems belonging to National Security Agency (NSA), FBI, DoD, and DHS.[42] DHS Secretary Janet Napolitano reaffirmed the importance of this effort with the creation of a new National Cybersecurity and Communications Integration Center (NCCIC). In addition to its previous mission, it now includes "watch and warning" for incidents and threats that affect the nation's critical information technology and cyber infrastructure.[43] In May of 2010, the DoD created the first U.S. Cyber Command (CYBERCOM) and the first U.S. CYBERCOM Commander. These policies and agencies were implemented because of the increase in cyber attacks and threats against the military.[44] From these newly formed centers emerges national policies. In July 2011, DoD issued the Department of Defense Strategy for Operating in Cyberspace.[45] The White House has issued two policy papers, the Comprehensive National Cyber Security Initiative[46] and the International Strategy for Cyberspace.[47]

The *Comprehensive National Cyber Security Initiative* states that the President considers cyberspace to be of critical importance and appoints an executive branch cyber security coordinator.[48] Additionally, it outlines 12 components for strengthening and addressing the federal networks as well as critical infrastructure.[49] The 12 components

---

[42] Office of the Press Secretary, "Statement by Homeland Security Secretary Michael Chertoff on the Appointment of the Director of the National Cyber Security Center" [press release], March 20, 2008, http://www.dhs.gov/xnews/releases/pr_1206047924712.shtm (accessed August 18, 2011).

[43] Office of the Press Secretary, "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center" [press release], October 30, 2009, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm (accessed August 18, 2011).

[44] Office of the Assistant Secretary of Defense (Public Affairs), "DoD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander" [press release], May 21, 2010, http://www.defense.gov/Releases/Release.aspx?ReleaseID=13551 (accessed August 18, 2011).

[45] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: Department of Defense, 2011).

[46] White House, *The Comprehensive National Cybersecurity Initiative*, Policy (Washington, D.C.: White House, 2008).

[47] White House, *International Strategy for Cyberspace*.

[48] White House, *Comprehensive National Cybersecurity Initiative.*

[49] Ibid.

address the key areas. If all areas could be addressed as easily as they are identified, it would greatly help the effort to strengthen the cyber risk. One of the key components identified directly pertains to this area of inquiry, specifically regarding supply chain threats. The DoD *Strategy for Operating in Cyberspace* provided that the DoD create a new cyber command and a new cyber range testing ground for cyber security efforts to be tested and proven.[50] The policy stresses much of the information in the *National Cyber Security Strategy*, emphasizing partnerships and the need for a secure and robust network; again covering the critical areas.

The *International Strategy for Cyberspace*[51] outlines and reiterates a little of both the DoD *Strategy and the National Cyber Security Strategy*. It also addresses the critical nature of the Internet and the world dependence on it for global commerce and transnational connections.[52] Furthermore, it advocates collaboration and partnerships on a worldwide scale to keep the Internet safe and secure. Furthermore, the strategy advocates global policing and prosecution of groups that perpetuate either disruption or interference with Internet traffic. It takes adopts from the DoD *Strategy for Operating in Cyberspace* and states, "[t]he United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so."[53] The issuance of these three policies, two of which emerged from the White House, captures the significance that the government has placed on cyberspace. A large amount of research and thought has been devoted to the core ideas of these strategies, but they are primarily focused around the federal network.

Much has been written on cyber security policy and how experts suggest best strategies to combat cyber attackers. These would include cyber terrorists and any other party that is a potential threat to the homeland. However, I have been unable to find much information on the vulnerabilities of computer hardware. These vulnerabilities

---

[50] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

[51] Whitehouse, *International Strategy for Cyberspace*.

[52] Ibid.

[53] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

would be in the actual components themselves. One of the only articles I have found is "Old Trick Threatens the Newest Weapons,"[54] wherein Markoff talks about the potential threat of creating computer chips and hardware that has vulnerabilities built into it at the time of manufacture. He implies that 98 percent of all computer hardware is purchased and built outside of the United States and its sterility cannot be validated.[55] This concern has prompted the National Security Agency (NSA) to create its own manufacturing plant for the most sensitive equipment, but that amounts to less than two percent of the computers the government procures. Markoff suggests that hardware can be in effect a Trojan horse wherein it is procured and deployed and when the moment is right, an attack initiated.[56] The concern is that the compromised hardware can never be identified and acts as a sleeper until either it is signaled or the requisite time has passed for its job to be preformed.

Specifically, it is in this area that more research needs to be completed. The research that is available is very little and although acknowledged as a significant threat, it is not addressed adequately in policy or other documents.

D. CONCLUSION

There is extensive writing concerning cyber security. Most of this writing is related to malware and software attacks. There is little written with respect to the hardware itself, which may be the largest vulnerability. As explained above, the concept of cyber security as it relates to hardware is almost non-existent. There are many hardware vectors that can be exploited to produce vulnerabilities. The security phenomenon for hardware has only recently begun to be exposed and documented. Most of the literature describes a potential risk or outlines some possible threats, but there is little information available on specific documented incidents. A few things are beginning

---

[54] John Markoff, "Old Trick Threatens the Newest Weapons," October 27, 2009, *The New York Times*, http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all (accessed November 20, 2011).

[55] Ibid.

[56] Ibid.

to be written on this topic but not a lot on the hardware layer. For information on this, I will have to continue to look and perhaps correspond with some professionals for opinions.

There has been a great deal of interest, study, and reporting on hardware and recently the security implications. While there is a well-developed understanding on the topic, our understanding of current vulnerability for homeland security would be improved by further research on what the vulnerabilities are and how we can mitigate the threat. Identifying how we can prevent these threats, or at least understand them, will allow decision makers and agencies involved to be more proactive about this important topic.

THIS PAGE INTENTIONALLY LEFT BLANK

III. BACKGROUND: U.S. MICROCHIP INDUSTRY AND THE MOVE OVERSEAS

The U.S. microchip industry was established in the 1950s by Jack Kilby of Texas Instruments and Robert Noyce of Fairchild Semiconductor Corporation.[57] Kilby received the Noble Prize for physics in 2000 for his invention of the integrated circuit. Noyce perfected Kilby's concept and continued to develop the integrated circuit making significant strides that are still in use today. He ultimately left Fairchild and founded the Intel Corporation where he developed the modern day CPU, which is in most computers today.[58]

From these humble beginnings, the integrated circuit or microchip industry evolved into a world dominating technology industry in Silicon Valley, California. These companies, like many early U.S. companies, performed the entire manufacturing process at their plants, from the idea to the design and testing, then on to the procurement of the raw materials from other U.S. companies. Fabrication, assembly, and final testing would then transpire at which point the companies would then market and sell their products, and provide support, all in one shop.[59] This process had its ups and downs throughout the 60s and 70s, due primarily to labor and procurement issues, but significant innovation and developments were made in the microchip industry. The beginnings of the shift began in the 1960s with the heavier labor cost operations outsourced to a location in another part of the world that had cheaper labor.[60] As shareholders began to enjoy a taste of the new larger profits the companies were reaping from the lower cost of labor, more and more industry transferred offshore. This trend continued with other manufacturing moving offshore to also lower costs and increase profits.

---

[57] "The Integrated Circuit," May 5, 2003, http://www.nobelprize.org/educational/physics/integrated_circuit/history/ (accessed October 22, 2012).

[58] Ibid.

[59] Michael French, *US Economic History since 1945* (New York: Manchester University Press, 1997).

[60] Government Accounting Office, *Offshoring*.

The 1980s accelerated this shift due to a technology war with Japan. Japan was producing microchips equal to and in some cases superior to the quality of the ones being produced in the U.S. but at prices below the cost of production. To stay competitive U.S. microchip companies had to adapt and continue to develop, but they also had to cut costs.[61] This movement continued to gain momentum as corporations found not only lower labor costs but also lower materials costs due to not having to ship to the U.S. Through the evolving manufacturing process, companies learned that they could save more money by outsourcing to companies that specialize in particular products rather than maintain the overhead of a company owned plant. By doing this, the costs fell even more, again increasing profit margins.[62]

The developing countries that hosted these industries embraced them, offering many tax breaks and other subsidies to entice their businesses. On the darker side, the companies did not have to pay high wages or concern themselves with regulations regarding salary, working conditions, pollution, or anything they had to contend with in the U.S. Additionally, the companies had access to a higher skilled and educated workforce that was capable of performing any task that was asked of them.[63] This was a mutually beneficial proposition for them.

The paradigm shifted for the microchip industry with two things, the Internet and the rise of the wafer fabrication foundries. These were new and specialized manufacturing facilities, owned by companies offshore, full of cutting edge microchip manufacturing equipment that the for which individual U.S. microchip companies did not have to spend capital. The Internet allowed for the immediate contact and transfer of data across the globe in an instant. It was as if the offshore location was not as far.

---

[61] Spencer Michaels, *The Growth of the Microchip* [PBS interview by Jim Lehrer online], January 1, 1993, *PBS Newshour*, http://www.pbs.org/newshour/bb/business/jan-june93/chip_1-1-93.html (accessed October 1, 2012).

[62] David Barboza, Peter Lattman, and Catherine Rampell, "How the U.S. Lost Out on iPhone Work," *New York Times*, January 21, 2012.

[63] Ibid.

Additionally, the cost for the new foundries was now spread over all of the companies that used them. This new way of production reduced the U.S. microchip production share to 20 percent.[64]

This trend in offshore fabrication has continued due to the newer technological challenges of the cutting edge designs and capabilities of the new microchips. These new products require new and advanced fabrication facilities. What could be accomplished in some of the older fabrication facilities is no longer relevant in the new environment. These new facilities cost even more than the predecessors, which make the option for in-house manufacture insurmountable for an individual company.[65] Add to this an ever-increasing demand for product—because now everything from cars to weapons requires microchips to function.

There are still a few companies that are known as integrated device manufacturers, meaning they have the capability to complete the production of a microchip. However, even though they can produce microchips, they are only doing so for older models. They are outsourcing the newer designs to an offshore foundry. Many of these companies are ones that are thought of as U.S. companies, "made in the USA;" however, that may not be the case as seen in Table 1. The U.S. government contracts for sensitive hardware with IBM, which owns a "trusted" foundry in Vermont for manufacturing those products.[66] However, this foundry cannot serve the needs of the entire government, especially regarding some of the specialty or newest designs.

Table 2 is a listing of various manufacturers, their production model and the locations of their corporate offices. Many are thought to be "made in the USA" companies, but in reality they are not. This issue can become more convoluted because many of these corporations buy companies or have subsidiaries that can do business for the production of microchips with one of the outsourcing companies. One example is

---

[64] Government Accounting Office, *Offshoring*.

[65] Ibid.

[66] Richard McCormack, "$600 Million Over 10 Years for IBM's 'Trusted Foundry' Chip Industry's Shift Overseas Elicits National Security Agency, Defense Department Response," *Manufacturing and Technology News*, February 3, 2004, http://www.manufacturingnews.com/news/04/0203/art1.html (accessed October 23, 2012).

Microsemi SoC Products Group. This company is a leading provider of field programmable gate array (FPGA) microchips to the U.S. government and is discussed in greater detail later in the paper. They are not on the trusted foundry list, however they are a "partner" of companies that are and purport to provide microchips to the military and aerospace industries.[67]

Table 2. 2011 Top 25 Fabless Integrated Circuit Suppliers[68]

2011 Top 25 Fabless IC Suppliers ($M)

2011 Rank	2010 Rank	2009 Rank	Company	Headquarters	2009 ($M)	2010 ($M)	% Change	2011 ($M)	% Change
1	1	1	Qualcomm	U.S.	6,409	7,204	12%	9,910	38%
2	2	3	Broadcom	U.S.	4,271	6,589	54%	7,160	9%
3	3	2	AMD	U.S.	5,403	6,494	20%	6,568	1%
4	6	5	Nvidia	U.S.	3,151	3,575	13%	3,939	10%
5	4	6	Marvell	U.S.	2,690	3,592	34%	3,445	-4%
6	5	4	MediaTek	Taiwan	3,500	3,590	3%	2,969	-17%
7	7	7	Xilinx	U.S.	1,699	2,311	36%	2,269	-2%
8	8	10	Altera	U.S.	1,196	1,954	63%	2,064	6%
9	9	8	LSI Corp.	U.S.	1,422	1,616	14%	2,042	26%
10	10	11	Avago	Singapore	858	1,187	38%	1,341	13%
11	13	12	MStar	Taiwan	838	1,065	27%	1,220	15%
12	11	13	Novatek	Taiwan	819	1,149	40%	1,198	4%
13	15	16	CSR	Europe	601	801	33%	845	5%
14	12	9	ST-Ericsson*	Europe	1,263	1,146	-9%	825	-28%
15	16	15	Realtek	Taiwan	615	706	15%	742	5%
16	17	17	HiSilicon	China	572	652	14%	710	9%
17	27	67	Spreadtrum	China	105	346	230%	674	95%
18	19	19	PMC-Sierra	U.S.	496	635	28%	654	3%
19	18	14	Himax	Taiwan	693	643	-7%	633	-2%
20	21	—	Lantiq	Europe	0	550	N/A	540	-2%
21	33	30	Dialog	Europe	218	297	36%	527	77%
22	22	21	Silicon Labs	U.S.	441	494	12%	492	0%
23	29	20	MegaChips	Japan	445	337	-24%	456	35%
24	23	24	Semtech	U.S.	254	403	59%	438	9%
25	24	23	SMSC	U.S.	283	397	40%	415	5%
Top 25 Total			—	—	38,242	47,733	25%	52,076	9%
Non-Top 25 Fabless			—	—	11,091	14,781	33%	12,811	-13%
Total Fabless			—	—	49,333	62,514	27%	64,887	4%

*Represents the 50% share not accounted for by ST.

Source: Company reports, IC Insights' *Strategic Reviews Database*

Table 3 is the top list of the fabless foundries, meaning the company designs and outsources fabrication.

[67] Microsemi SoC Products Group, *Microsemi SoC Products Group—Partners*, 2012, http://www.actel.com/products/partners/solution/ip/specialization.aspx (accessed November 8, 2012).

[68] "U.S.-based Companies Held 12 of the Top 25 Fabless Spots in 2011," IC Insights, 2011, http://www.icinsights.com/news/bulletins/USbased-Companies-Held-12-Of-The-Top-25-Fabless-Spots-In-2011/ (accessed October 23, 2012).

Table 3. 2011 Major Integrated Circuit Foundries[69]

2011 Major IC Foundries

2011 Rank	2010 Rank	Company	Foundry Type	Location	2009 Sales ($M)	2010 Sales ($M)	10/09 Change (%)	2011 Sales ($M)	11/10 Change (%)
1	1	TSMC	Pure-Play	Taiwan	8,989	13,307	48%	14,600	10%
2	2	UMC	Pure-Play	Taiwan	2,815	3,965	41%	3,760	-5%
3	3	GlobalFoundries	Pure-Play	U.S.	1,101	3,510	219%	3,580	2%
4	5	Samsung	IDM	South Korea	290	1,205	316%	1,975	64%
5	4	SMIC	Pure-Play	China	1,070	1,555	45%	1,315	-15%
6	6	TowerJazz	Pure-Play	Israel	300	509	70%	610	20%
7	7	Vanguard	Pure-Play	Taiwan	382	508	33%	519	2%
8	8	Dongbu	Pure-Play	South Korea	378	475	26%	500	5%
9	9	IBM	IDM	U.S.	335	430	28%	445	3%
10	10	MagnaChip	IDM	South Korea	262	405	55%	350	-14%
11	12	SSMC	Pure-Play	Singapore	280	330	18%	345	5%
12	11	Hua Hong NEC*	Pure-Play	China	240	367	53%	335	-9%
13	16	WIN	Pure-Play	Taiwan	145	221	52%	300	36%
14	13	X-Fab	Pure-Play	Europe	212	317	50%	285	-10%
—	—	Chartered**	Pure-Play	U.S.	1,540	0	N/A	0	N/A

*Merging with Grace in 2012.
**Purchased by GlobalFoundries in 4Q09.

Source: IC Insights, company reports

Table 4 is a list of the top foundries, meaning they manufacture for anyone.

69 "2011Major Integrated Circuit Foundries" [Strategic Reviews Database, company reports], *IC Insights*, 2011.

Table 4. Top Foundries Worldwide: Headquarter Location and Manufacturing Location[70]

Manufacturer	Headquarters Location	Semiconductor Fabrication and Assembly*
Fairchild	USA	China, South Korea, Malaysia, Philippines, United States
Fujitsu	Japan	China, Japan, United States
GSI Technology	USA	Taiwan
IBM	USA	Canada, Japan, United States
IDT	USA	Taiwan, United States
Intel	USA	China, Germany, Ireland, Israel, United States
Xicor (now Intersil)	USA	China, Netherlands, United States
Lattice	USA	China, Japan, South Korea, Malaysia, Philippines, Taiwan
Motorola	USA	Mexico, Malaysia
National Semiconductor	USA	Malaysia, United Kingdom, United States
NEC	Japan	China, Japan
Pericom Semiconductor	USA	China, Taiwan
Pulse Electronics	USA	China
Samsung	Republic of Korea	China, South Korea, United States
STMicroelectronics	Switzerland	China, France, Italy, Morocco, Malta, Malaysia, Philippines, Singapore
Texas Instruments	USA	China, Germany, Japan, United States
		* Fabrication and packaging/assembly partner locations, where applicable

An example of a company that went off shore is the National Semiconductor Corporation. This company was established in 1959, in the beginning of the microchip

[70] Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington, D.C.: Northrop Grumman Corp., 2012).

era in Silicon Valley. It is still a leading U.S. manufacturer of semiconductors used in many electronics applications; however, during the Asian price wars in the 1980s the company, as many others, entered a severe downturn. The decline was so severe the company asked Washington to impose trade sanctions against the Japanese.[71] The company survived and was one of the first companies to move its assembly operation offshore in an effort to save money and reestablish itself. This business decision proved beneficial and National Semiconductor returned to profitable status. It went on to buyout several other competitors, including Fairchild Semiconductor and Cyrix, and later established a fabrication foundry in China.[72] Recently, it has partnered with Taiwan Semiconductor Manufacturing Corporation (TSMC), the largest producer of microchips in the world. Although this microchip producer has a history and a presence in the U.S., it is in reality a foreign company.

Another surprising company that changed its corporate structure to the offshore outsourcing model is Texas Instruments (TI). Founded in 1951 in Dallas, Texas, it is credited with having the inventor of the first integrated circuit; Jack Kilby employed there. The company has a long and storied relationship with the military, having provided military computers, armament, and radar systems. But semiconductor production makes up the majority of the businesses revenue. In fact, TI has bought out nine other semiconductor companies. Despite the lucrative contracts from the military, TI also encountered the cash flow issues in the 1980s, which resulted in the company merging with the Japanese firm Hitachi to develop a new microchip. This move helped restructure and save the company. As a part of the restructuring and cost reduction, it moved some of its fabrication to a foundry in Singapore in 1991. To date, it has

[71] Bryan T. Johnson, "The Heritage Foundation Research: Asia," The Heritage Foundation, January 24, 1991, http://www.heritage.org/research/reports/1991/01/bg805-the-us-japan-semiconductor-agreement (accessed November 8, 2012).

[72] Jonathan Martin, David Salamie, Nelson Rhodes, "National Semiconductor Corporation," *International Directory of Company Histories*, 2005, http://www.encyclopedia.com/doc/1G2-3429600082.html (accessed November 8, 2012).

continued to invest heavily in the fabrication industry in Asia, pledging to invest a billion dollars in manufacturing.[73] TI is another example of a U.S. rooted company that has extremely deep ties to foreign interests.

As can be seen in Tables 1 through 3, many microchip companies, which are thought of as manufacturing within the U.S., have their fabrication done at offshore facilities. Others have links to the offshore industry through various business relationships. The primary driving force for the exodus of the microchip manufacturing process is profit. This situation, however, creates a significant vulnerability to national security through the use of these microchips in critical systems when they are manufactured in countries that are not allies of the U.S.

[73] "Texas Instruments Inc.," *International Directory of Company Histories*, 2002, http://www.encyclopedia.com/doc/1G2-2845000111.html (accessed October 23, 2012).

IV. MANUFACTURING OF MICROCHIPS IN CHINA: IMPLICATIONS AND CONSIDERATIONS

China and Taiwan supply the majority of the microchips imported by the United States government Department of Defense and private industry with more than two-thirds market.[74] There is a concern that microchips manufactured in China and purchased by the U.S. government may contain a manufactured vulnerability. Dr. William Howard, Task Force Chairman of the 2005 Defense Science Board Task Force on High Performance Microchip Supply, stated, "Our greatest concern lies in microelectronics supplies for defense, national infrastructure and intelligence applications.…Urgent action is recommended…"[75] This was due to the findings of the task force regarding identified vulnerabilities in the supply chain.[76]

Additionally, the Emerging Cyber Threats Report for 2012, put together during the Georgia Tech Cyber Security Summit, identifies hardware as an emerging threat.[77] More specifically, it claims that threats are becoming embedded in the hardware that modify the basic input/output system BIOS.[78] These threats come via the hardware supply chain. According to Andrew Howard, research scientist at Georgia Tech Research Institute:

> Twenty years ago when power stations weren't IP enabled, that may have been less of a concern. But now that we are phasing out legacy hardware for newer equipment that is connected to the Internet, it could open a vulnerability to something like Stuxnet.[79]

---

[74] Defense Science Board, *High Performance Microchip Supply*.

[75] Ibid.

[76] Ibid.

[77] Georgia Tech University, *Emerging Cyber Threats Report 2012* (Atlanta, GA: Georgia Tech University, 2011), Summary.

[78] Ibid.

[79] Ibid.

The new concern is that perhaps there is another layer of vulnerability out there, one at the hardware layer. One that is hard coded and cannot be corrected without the replacement of the corrupt part—a microchip that has a purposeful manufactured vulnerability.

Much is been written on the speculation that China or others are manufacturing microchips and other computer electronics that have back doors and trojans within them;[80] however, so far there are no unclassified reports of any vulnerabilities exploited by the Chinese or others. Supply chain vulnerability has been well documented and the definitive document is from the 2005 Defense Science Board Task Force on *High Performance Microchip Supply Report*, which identifies the possibility for a supplying country to curtail production as a means to impact the outcome of a conflict.[81] It also identifies the possibility for the purposeful manufacturing of vulnerabilities.[82] Specifically, the Defense Science Board (DSB) warned that the shift towards greater foreign circuit production posed the risk that "trojan horse" circuits could be unknowingly installed in critical military systems. The DSB warned that foreign adversaries could modify chips to self destruct or add secret back doors that would place a kill switch in military systems.[83] However, to date, few of the recommendations in the report have been implemented to avoid the identified vulnerabilities.

In a War College thesis titled Semiconductor Technology and U.S. National Security, Colonel (COL) Lawerence K. Harada wrote about the concerns associated with transfer of the semiconductor (microchip) industry from the U.S. to China.[84] That "[t]his transfer is a national security concern and the U.S. must regain worldwide leadership semiconductor technology to maintain a technological advantage over other adversaries."

---

[80] John D. Villasenor, "Ensuring Hardware Cybersecurity," *Issues in Technology Innovation*, no. 9 (May 2011); Mike Rogers and Charles Albert Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Washington, D.C.: House of Representatives, 2012).

[81] Defense Science Board, *High Performance Microchip Supply*.

[82] Ibid.

[83] Ibid.

[84] Lawrence K. Harada, *Semiconductor Technology and U.S. National Security* (Carisle, PA: U.S. Army War College, 2010).

He specifically states that current export policies to China have failed, and they must be aggressively addressed because of the loss of intellectual property.[85]

In addition, numerous reports have identified the supply chain threats. "The main threat to product trustworthiness is the intentional inclusion or insertion of exploitable vulnerabilities, backdoors or malicious logic,"[86] says a State of the Art Report (SOAR) prepared by the Information Assurance Technology Analysis Center (IATAC) on Security Risk Management for Off-the Shelf (OTS) Information and Communications Technology (ICT) Supply Chain. Additionally, numerous threats to the ICT supply chain are identified and the potential impact to the DoD and all government agencies are detailed. The report suggests several options to mitigate the threat as it exists today and offers some suggestions for future strategies as well.[87]

There is no empirical data regarding microchip or hardware compromise; however, much what exists is with respect to supply chain vulnerability issues.[88] There are numerous documented instances of hacking or theft of intellectual property.[89] The aggressiveness and increased instances of unclassified attacks on federal government computer systems, DoD systems and federal contractor systems continues to rise, with the majority coming from Eastern Europe and Asia.[90] Therefore, it can be hypothesized that new vectors for attack will be identified and that hardware or microchip vulnerability could be exploited if the attacker had knowledge of it.

David M. Abel and Kyle I. Fox conducted a detailed analysis of documented unclassified supply chain incidents from 1988 to 2011. They found in the majority of the

---

[85] Harada, *Semiconductor Technology.*

[86] Kristy Mosteller, Holly McKinley Schmidt, Stephanie Shankles, and Theodore Winograd Karen Goertzel, *Security Risk Management for the Off-the Shelf (OTS) Information and Communications Technology (ICT) Supply Chain* (Herndon, VA: Information Assurance Technology Analysis Center, 2010).

[87] Mosteller et al., *Security Risk Management for the Off-the Shelf.*

[88] Defense Science Board, *High Performance Microchip Supply*.

[89] Michael Riley and Ashlee Vance, "It's Not Paranoia if They're Stealing Your Secrets," *Bloomberg Business Week*, March 19, 2012.

[90] Alexander Hutton Wade, C. David Hylendar, Joseph Pamula, Christopher Porter, and Marc Spitler Baker, *2011 Data Breech Investigations Report* (New York: Verizon, 2011), Summary.

183 incidents that the vendor or subcontractor took responsibility for the supply chain malware; however, that does not mean they were responsible for the inclusion, only that they took responsibility.[91] There was only one verifiable instance attributed to a nation state in their unclassified report.[92] This is surprising, considering what has been written regarding the potential for exploitation by nation states.[93] Their analysis also showed that although the vendor or subcontractor took responsibility, there are still unanswered questions as to who perpetrated the attack and why; there were also a large percentage that were attributed to "unknown."[94] Some potential reasons for this could be the lack of trusted oversight or trusted quality control in the process. Finally, if we add the incidents that responsibility was taken with the "unknown," the total number of incidents is by far the majority, so further analysis is warranted in this area.

Appendix A details significant cyber incidents since 2006 to present as collated by James Andrew Lewis of the Center for Strategic and International Studies. Of course, these are incidents that have become known and are not classified. See Figure 1.

[91] David M. Abel and Kyle I. Fox, *Sleeper Cells in Cyberspace: Analyzing Supply Chain Malware Incidents for Offensive and Defensive Implications* (master's thesis, Naval Postgraduate School, 2011).

[92] Ibid.

[93] Defense Science Board, *High Perfromance Microchip Supply*.

[94] Abel and Fox, *Sleeper Cells in Cyberspace*.

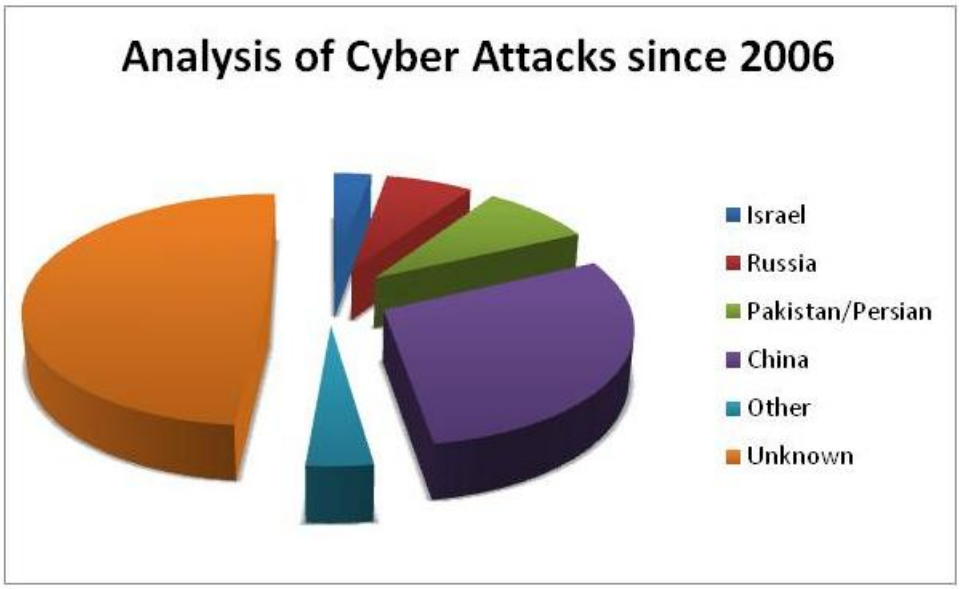

Figure 1. Breakdown of Cyber Attacks since 2006[95]

As can be seen in Figure 2 there has been a steady increase in cyber attacks since 2006, the majority (Figure 1) of which can be attributed to an attacker with a Chinese origin (57 percent of identified attacks and 30 percent of all).[96] These are discounting the unknown attacks, which account for 47 percent of the total.[97] These numbers are significant in they clearly show a pattern that cyber attacks are not only on the rise, but that hackers in China are the number one point of origin. The numbers also demonstrate that if they are attacking, they will exploit any vulnerability they can, including those purposefully manufactured in a microchip.

[95] James Andrew Lewis, *Significant Cyber Events Since 2006* (Washington, D.C.: Center for Strategic and International Studies, 2012).

[96] Ibid.

[97] Ibid.

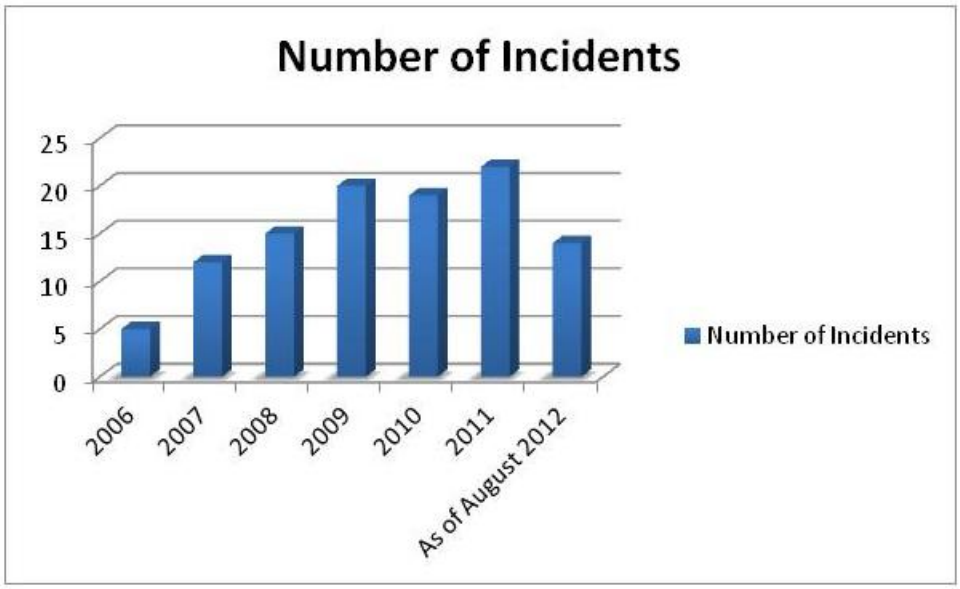

Figure 2. Number of Significant Incidents by Year[98]

According to Verizon, which conducts an annual study in conjunction with the United States Secret Service (USSS) into data breech investigations, 92 percent of the breeches reported were from external agents with 73 percent exploiting a backdoor or control channel.[99] This is significant because it validates the concern regarding the potential for someone to exploit a backdoor in a microchip. See Figure 3.

[98] Lewis, *Significant Cyber Events Since 2006*.

[99] Hutton Wade et al., *2011 Data Breech Investigations Report*.

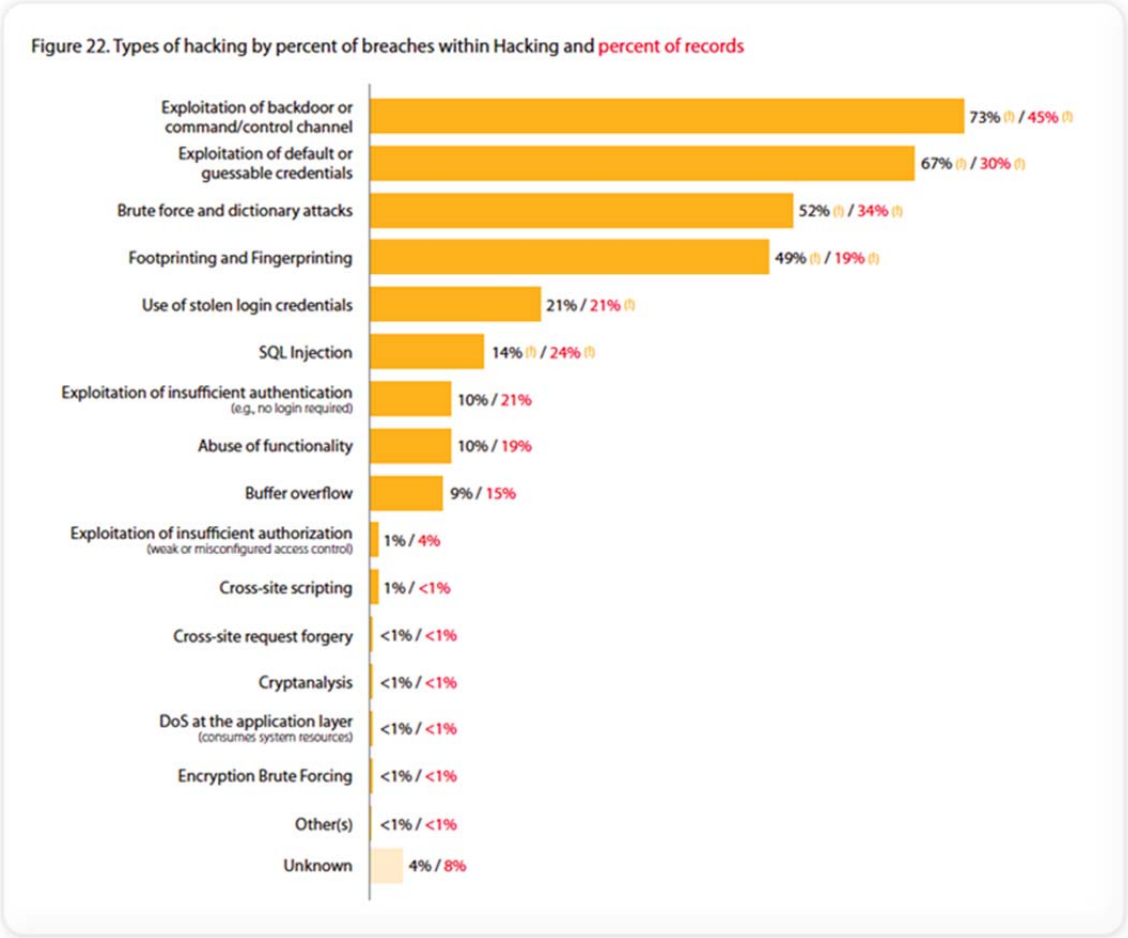

Figure 3. Types of Hacking by Percent of Breeches[100]

Greg Schaffer, Acting Deputy Undersecretary at the Department of Homeland Security's National Protection and Programs Directorate, testified before the House Oversight and Government Reform Committee in July of 2011. When asked by Representative Chaffetz whether he was aware of any foreign-manufactured software or hardware components that had been purposely embedded with security risks, the DHS representative stated that "I am aware of instances where that has happened."[101] Though he did not elaborate or cite what type of equipment was compromised, he did say that

[100] Hutton Wade et al., *2011 Data Breech Investigations Report.*

[101] Neal Ungerleider, "DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools," *Fast Company*, July 7, 2011, http://www.fastcompany.com/1765855/dhs-imported-consumer-tech-contains-hidden-hacker-attack-tools (accessed October 10, 2012).

foreign components are in many "American" manufactured devices.[102] This statement is significant because it is one of the first public acknowledgements by a high-ranking government official of this issue.

As previously stated there have been numerous instances of malware being embedded in a device, only later identified. However there has been no unclassified acknowledgement of instances where a microchip or the hardware was identified with a manufactured vulnerability. The concerns about a purposefully manufactured vulnerability, and statements such as these, have prompted investigations by various committees in the House and Senate. One such investigation is being conducted by Representative Mike Rogers (R-Michigan), the chairman of the House Permanent Select Committee on Intelligence. The committee was looking into the possibility for the Chinese government to tamper with telecommunications equipment, thereby allowing it to spy, threaten our critical infrastructure, or obtain intellectual property from the U.S. [103]

[102] Ungerleider, "DHS: Imported Consumer Tech."

[103] Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues.*

V. THE MICROCHIP: ITS USE, MISUSE, AND INSPECTIONS

A. USE

A microchip is defined as a small silicon wafer or integrated circuit.[104] Each microchip has a designed function to perform in relation to a larger operation. An analogy to this would be a gear in a watch. The gear provides a specific function within the watch and without it the watch may not function correctly, if at all. The microchips are put together on a board to perform a process. An example of a process would be to go into sleep mode or enter into a wireless mode. Microchips are in most electronic devices, from cars to computers, from weapons to refrigerators. They provide a specific action to be taken once power is applied to them, before any software or operating system engages. They start the software, which is why a purposefully manufactured vulnerability in a chip is so dangerous; it cannot be caught by antivirus or malware programs.

Actel/Microsemi ProASIC3 FPGA, which is sold by Microsemi SoC Products Group and is manufactured offshore in Taiwan by United Microelectronics Corporation (UMC),[105] is an example of a microchip that is in use today by the military[106] in critical infrastructure and in commercial aviation. According to the manufacturer's Website, this particular microchip is used by the military and in avionics systems, such as mission computers, navigation, and guidance systems. All of these are critical systems. In commercial aviation, it is used in the new Boeing 787 Dreamliner. The military is extremely reliant on this particular type of microchip because of the flexibility that it

[104] Techterms Computer Dictionary, s.v., "integrated circuit," http://www.techterms.com/definition/integratedcircuit (accessed November 8, 2012).

[105] "Actel Leverages UMC Foundry Solutions for 65nm eFlash FPGAs," *Design and Reuse News*, November 18, 2008, http://www.design-reuse.com/news/19553/65nm-eflash-fpga.html (accessed November 8, 2012).

[106] Gwen Carlson, "Actel Expands Military-Qualified Flash-Based FPGA Offerings" [press release], Microsemi Soc Products Group, August 11, 2008, http://www.actel.com/company/press/2008/8/11/ (accessed November 8, 2012).

offers. It allows the chip to be programmed to perform whatever task required, often being referred to as a "glue chip," one that functions as the core for all else to be attached to.[107]

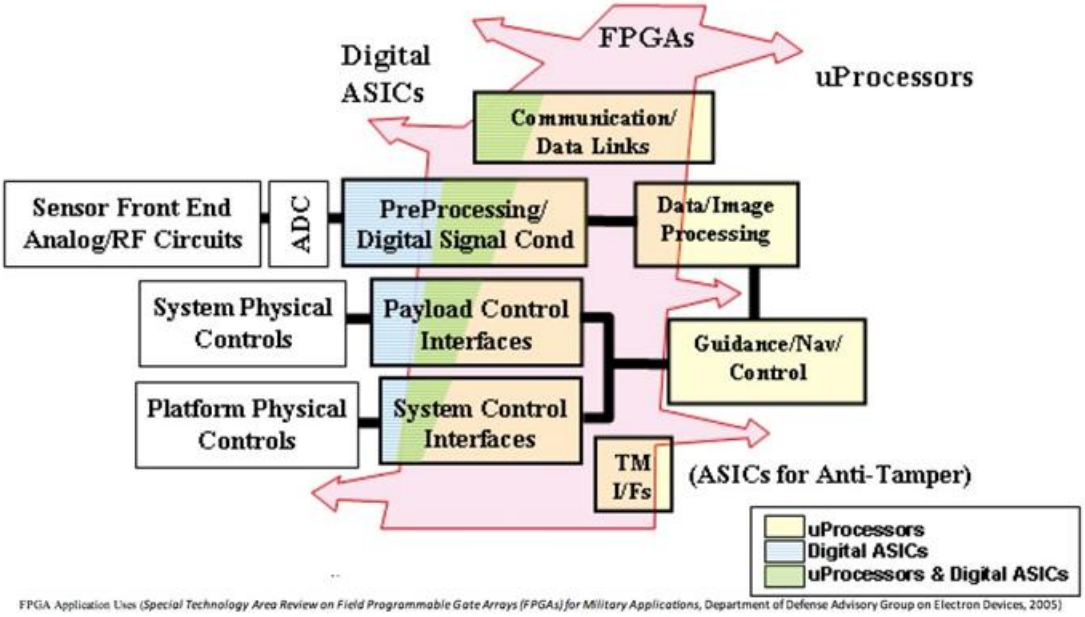

Figure 4. FPGA Application Uses[108]

Another example is the microchips produced by Intel for use in computers, servers, and mobile devices as well as other types of peripherals, including motherboards.[109] These microchips are in use in approximately 80 percent of personal computers worldwide,[110] which include the military and government at all levels. In

[107] Office of the Under Secretary of Defense Acquisition (Technology & Logistics), *Special Technology Area Review on Field Programmable Gate Arrays (FPGAs) for Military Applications* (Washington, D.C.: Department of Defense Advisory Group on Electron Devices, 2005).

[108] Ibid.

[109] "Intel," Intel Corporation, http://www.intel.com/content/www/us/en/homepage.html# (accessed November 8, 2012).

[110] International Directory of Company Histories, s.v. "Intel Inc.," 2002, http://www.encyclopedia.com/topic/Intel_Corp.aspx (accessed November 8, 2012).

2010, Intel opened a new fabrication facility in China, but it has operated assembly and testing facilities in China, Malaysia, and Vietnam since 2005. These are two examples of uses of microchips and their manufacturers' practices.

B. MISUSE

So how exactly would something like manufactured hardware vulnerability work? What could it do? Before answering these questions, it is important to note that unlike software, which can be updated to correct issues or problems with the programming code, hardware is designed and manufactured with the built-in code. For the most part, this code cannot be changed or corrected after the microchip leaves the factory. The only way to address the issue would be to replace the compromised unit with an uncompromised one. Once the compromised microchip leaves the factory, there are numerous ways that a vulnerability could be exploited on whatever system it was installed. A certain date or physical location could wake the process up, at which point it would execute the preprogrammed attack. Like a sleeper, it could be waiting for a certain number of days before it executes or even a call from the owner. Of course, the latter would be predicated on access to the Internet or a phone line. The type action that could be taken can be anything from a backdoor allowing remote access to systems to an automated download of classified data or even a remote kill switch that would shut off whatever system the microchip was in.[111]

An example of this type of exploit would the Flame attack on the computer networks of Iran. Flame installed itself on the host computer and then opened a backdoor and called home for further instruction and to download information that it had initially gathered from the host.[112] This is very significant because nearly every military or governmental system today utilizes some type of commercially manufactured microchip.

There are two basic points in the microchip production process that are vulnerable to attack; the design phase and the fabrication phase. For the most part, a microchip is

---

[111] John Villasenor, "The Hacker in Your Hardware," *Scientific American* 303, no. 2 (2010): 82–88.

[112] Kim Zetter, "Meet 'Flame,' the Massive Spy Malware Infiltrating Iranian Computers," *Wired Magazine*, May 12, 2012.

designed for a particular use and as such requires a design and building plan. These plans are then checked to ensure that they meet the requirements and specifications at which point they are given to the fabrication foundry where the chips are actually made. Today, these two processes are oftentimes split with the design done in the U.S. by the microchip company. The design plan is then sent to the foundry offshore where the microchips are fabricated. The highest probable attack vector would be in the design phase. This is because all designs have to be logic tested to ensure that they work properly. If a malicious process was embedded, it would have to be tested logically to ensure it is compatible with the rest of the process on the microchip. It is much easier to see how a malicious process will function in a computer testing environment than trying to see if it works after being introduced during fabrication.[113] During the design phase, the malevolent actor can disguise the process as legitimate and the plan can be modified to accommodate the malicious code and ensure compatibility in functionality, only now with the vulnerability included.

During the fabrication process, a modification is more difficult because the logic on the microchip has already been validated with the initial design. Therefore, any addition to the microchip at that point could cause a conflict and render the chip inoperative or impact the functionality in some way that would flag it as a problem. At that point, the microchip would be scrutinized to determine what causes the problem and the malicious process could be identified. This is not to say that a microchip could not be compromised at this point in the process, but it would be a little more difficult. One way that this could be accomplished would be to obtain a functional, unmodified microchip that could then be reverse engineered so that the malicious actors could insert a modification and vet it to ensure it does not impact the functionality. Once that is determined, an additional step could be taken during the manufacturing process to insert the vulnerability on all subsequently fabricated microchips. Regardless of the source, once a microchip has been manufactured with vulnerability the likelihood of it being identified is almost nil.[114]

[113] Villasenor, "Ensuring Hardware Cybersecurity."

[114] Ibid.

According to Sergei Skorobogatov of Cambridge University, not only does the threat exist, but he has found backdoors on existing chips.[115] He recently developed a non-invasive/non destructive testing process for microchips called pipeline emission analysis and tested a commercial off the shelf field programmable gate array (FPGA) chip (see Figure 5).[116] This is the most commonly used chip type by defense contractors. End users such as the DoD like this chip because, though it has basic functionality programmed into it, it highly customizable to the individual need via a software layer. Because it is a multi-use chip, it comes with many transistors that may not be needed for the particular use, thereby providing multiple opportunities to embed a malicious process, which would be almost impossible to find. Skorobogatov and Cambridge University are the first researcher/research institution that has successfully tested off the shelf Actel/Microsemi ProASIC3 FPGA in current use today and found a preprogrammed backdoor in the silicon of a microchip itself. This particular chip was chosen because of its high security specifications and widespread military use. From the manufacturers product information says "…offers one of the highest levels of design security in the industry."[117]

All levels of security were evaluated and each was able to be circumvented. Additionally, they were able to extract the secret key to activate the backdoor, as well as other security keys for the device.[118] Through the use of this vulnerability, a malicious actor could extract all of the data from the chip, reprogram it, or even permanently damage the device. In pursuing any of these options, the actor could then open other backdoors on the system if it is installed on or even take any information he or she wanted.

Their discovery was important in two ways. First, it was non invasive, and second, it confirmed what many had suspected, vulnerability is being manufactured in the

---

[115] Skorobogatov and Woods, *Breakthrough Silicon Scanning Discovers Backdoor*.

[116] Ibid.

[117] "Actel ProASIC3/E Production FPGAs, Features and Advantages," Microsemi SoC Products Group, 2007, http://www.actel.com/documents/PA3E Tech WP.pdf (accessed October 21, 2012).

[118] Skorobogatov and Woods, *Breakthrough Silicon Scanning Discovers Backdoor*.

microchips and the supply chain has been compromised by the introduction of these vulnerable chips. The implications of this finding are very significant[119] because the backdoor exists on the silicon itself and not any firmware loaded on the chip. Additionally, Skorobogatov is concerned that since this type of chip is designed for "secure" remote access, it would be possible for an attacker to initiate a large scale remote attack via the Internet. Other products from Actel/Microsemi were analyzed and all were found to have the same backdoor.[120] This raises serious questions about the integrity of the manufacturers and their respective security practices. As previously stated, having a hardware vulnerability negates any attempt at security through software because the attacker can always circumvent the system through the most base layer, the hardware. As a result of these findings, decisions will have to be made as how to remediate what is already in production and how security is enforced in future production.[121]

[119] Skorobogatov and Woods, *Breakthrough Silicon Scanning Discovers Backdoor*.

[120] Ibid.

[121] Ibid.

The ProASIC3 evaluation board hosts an A3PE600 device in a PQ208 package. It is programmed using the USB-based FlashPro3 JTAG emulator. Most of the on-board peripherals are jumper selectable, allowing easy reconfiguration.

Figure 5. An Example of a Field Programmable Gate Array (FPGA)[122]

C. CURRENT QUALITY CONTROL PROCESSES AND ASSOCIATED CHALLENGES

As stated above, the microchip fabrication process is twofold. The first phase is the design phase and the second the fabrication phase. During each phase, there are extensive quality control processes to ensure that the microchips not only function but function correctly. One could easily think "aha, this is the step where the vulnerabilities will be found," not necessarily. During the design phase, the chip functionality is designed and worked out on a computer aided design or CAD software. The software ensures the compatibility and functionality for what processes the microchips are being designed to perform. There can be as many as a million gates or more on a microchip

[122] William Wong, "Electronic Design," September 7, 2006, http://electronicdesign.com/article/embedded/eied-online-fpga-3-actel-proasic-starter-kit13423 (accessed October 8, 2012).

making extensive testing for security all but impossible.[123] The "bugs" are tested for and there are some random tests conducted periodically, but it is easy to hide a malicious process behind another that would never be discovered. It is for this reason that, for the most part, the design process is conducted in the microchip company's home base where they have more control. However, it is at this stage that the process is most vulnerable.[124]

The fabrication phase is outsourced, usually offshore or elsewhere where the costs are minimized. An attack at the fabrication phase is more difficult because a change to the hardware could adversely impact the functionality of the microchip and be identified during a quality control process. However, it could be accomplished if the chip design was obtained and the change was logically checked to ensure the functionality. It could also be introduced in a regularly manufactured microchip that had been reversed engineered and the functionality checked with the added vulnerability.[125] The process would at that point again be the same with respect to the introduction to the supply chain; they would then be introduced and consumed by the intended users.

The largest issue that is being confronted by microchip consumers is the difficulty in testing to validate integrity. Current technology uses several methods to validate the integrity of microchips. All of these are extremely time consuming and expensive to conduct, and most are destructive. The first method involves applying x-ray technology to the chip. This method can be destructive if the x-rays are too strong; furthermore, it can be difficult to discern the functionality of specific circuits. However, a company in California is building nondestructive x-ray microscopes that are already used and is experimenting with its use for security purposes. The second method is reverse engineering. This requires grinding the chip down layer by layer, and taking photos of the process via an electron microscope until the entire chip is imaged. The images of the chip can then be compared to the originally designed microchip. Also, each individual circuit's functionality can be scrutinized to determine what process it actually performs.

---

[123] Clive Maxfield, *The Design Warrior's Guide to FPGAs* (Burlington, MA: Elsevier, 2004).

[124] Ibid.

[125] Adee, "The Hunt for the Kill Switch."

This process is extremely labor intensive, destructive, and very expensive. It is not very reliable because manufacturers, designers, and malicious actors anticipate this will occur and build security measures into the chip to camouflage the functionality.[126] The third process involves some type of electrical monitoring. All microchips require electricity to function. Testing them for the amount of electricity used or their resistance and comparing those findings to a standard can identify a potential security flaw.[127]

Which one of these processes is the best at identifying an issue? They all have their respective shortcomings, and none of them can perform an absolute validation, but this is where technology in this field is currently. Obviously, each of these processes is incredibly laborious and cost prohibitive, as well as destructive. Thus far, there has been no microchip integrity validation process identified that is not destructive or cost prohibitive. This concern had led DARPA and IARPA to issue solicitations for proposals for new innovative ways to perform these validations.[128] This program has industry leaders attempting to identify malicious code inserted into microchips with a 90 percent probability.[129]

Many security-observers question whether a purposefully manufactured vulnerability could be built into hardware such as a microchip in a way that is not detected. According to research at the University of Illinois, it can be and was done.[130] The University of Illinois Computer Science Department sought to prove that it is possible to implant an undetectable vulnerability on a microchip. They then did it and provided the compromised chip along with uncompromised chips to researchers to see if they could determine, which was the compromised chip. This was done utilizing current technology. The researchers were not successful in finding the vulnerability so the

---

[126] Adee, "The Hunt for the Kill Switch."

[127] Youngjune L. Gwon, H. T. Kung, and Dario Vlah, "DISTROY: Detecting Integrated Circuit Trojans with Compressive Measurements," *6th USENIX Workshop on Hot Topics in Security (HotSec)* 36, no. 6 (December 2011).

[128] Adam Rawnsley, "Can Darpa Fix the Cybersecurity 'Problem From Hell?'" *Wired*, August 5, 2011.

[129] Adee, "The Hunt for the Kill Switch."

[130] Tucek et al., *Designing and Implementing Malicious Hardware.*

university was able to prove their point that it can be done.[131] The concern is significant enough to warrant DARPA and IARPA to begin initiatives to identify potential microchip vulnerabilities.[132] As stated previously, the current process for identifying compromised microchips is very difficult, time consuming and expensive. Even in doing so, the correct identification of a potential vulnerability is not a sure thing.

Only recently are governmental agencies looking seriously at the possibility of microchip vulnerability. According to Dr. Carl McCants, a Program Manager at DARPA, there have been no documented instances that a microchip has been compromised.[133] He went on to say there has been speculation and instances of malware being inserted on a platform, but nothing that can be attributed to this actually having occurred.[134]

[131] Tucek et al., *Designing and Implementing Malicious Hardware*.

[132] Federal Business Opportunities, "Integrity and Reliability of Integrated Circuits (IRIS)," https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=30191c1ba1db9c257723e48b97d4c155&_cview=0 (accessed January 28, 2012).

[133] Carl McCants (DARPA Program Manager), interview by author, February 15, 2012.

[134] Ibid.

VI. GOVERNMENT EFFORTS TO ADDRESS CYBER SECURITY IN CONJUNCTION WITH THE PURPOSEFULLY MANIPULATED MICROCHIP ISSUE

A paradigm shift is happening in cyber security that creates a change in tactics and policies. The cyber security community will adapt and evolve, just as it always has. The new threat is compromised hardware. One aspect of compromised hardware is the microchip. As we have discussed, microchips are not only vulnerable to the actors who were responsible for the purposefully manufacturing, but now this new vulnerability has been exposed and anyone with the right skill set can exploit it. This creates additional overarching cyber security concerns, with new vectors for attack that cannot be "patched" via a software upgrade. The "key" to these attacks has now been published, along with a how to guide; it will be only a matter of time before attacks begin.

Attacks on computer systems can range from disruption of critical infrastructure to financial gain, and now, even in the military theatre. The definition of cybercrime is criminal activity done using computers and the Internet.[135] This definition is very broad and growing more so each day as more illegal computer activities are being committed and identified. The economic impact is enormous and, as a crime, the impact on investigative resources will be significant as well. According to Symantec, a leading provider of internet security products, cybercrime cost victims $388 billion in time and money last year alone, hitting 431 million people in 24 countries.[136] That number is rising steadily; the 54 percent of online adults who were victims of computer virus or malware attacks this year is up from 51 percent last year.[137] Additionally, attacks against mobile devices are soaring as well. Findings show that 42 percent more smartphones,

[135] Techterms Computer Dictionary. s.v. "cybercrimes."

[136] Symantec, *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually* (Mountain View, CA: Symantec, 2011).

[137] Ibid.

tablets, and other mobile devices were targeted for malware attacks last year, as compared with 2009.[138] This is a clear indication that cybercrime is increasing and must be addressed.

Although the financial impact of cyber criminal activity and intellectual property theft cannot be completely quantified, the White House issued the *Cyber Security Policy Review*, which profiled the systemic loss of U.S. economic value from intellectual property and data theft in 2008 as high as one trillion dollars.[139]

Another concern for cybercrime investigators is a potential attack on critical infrastructure. For the most part, an attack on critical infrastructure would most likely be related to some type of terrorist activity, but it cannot be ruled out that it could be someone testing his or her hacking ability with no terrorism nexus at all. Cyber terrorism is a real and emerging threat in the homeland security arena, and it is gaining momentum daily. There are ever increasing groups and companies that are willing to provide destructive services to the highest bidder.[140] A small country or group with limited backing could potentially purchase a cyber weapon, deploy it, and cripple a target's critical infrastructure, financial system, or even military.[141]

Federal agencies report increasing cyber-intrusions into government computer networks, perpetrated by a range of known and unknown actors. Therefore, cyber security has become a pressing national security issue.[142] In fact, many national security experts have stated both in public and before various governmental committees that the United States infrastructure is vulnerable to cyber attack. The former Director of

---

[138] Symantec, *Norton Study Calculates Cost of Global Cybercrime*.

[139] Whitehouse, *Cyber Space Policy Review*.

[140] Riley and Vance, "Cyber Weapons: The New Arms Race."

[141] Ibid.

[142] John Rollins and Anna C. Henning, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations* (Washington, D.C.: Congressional Research Service, 2011), 2.

National Intelligence Mike McConnell stated that cyber weapons were equivalent to weapons of mass destruction if utilized by terrorists in an attack on the U.S. infrastructure.[143]

The Government Accounting Office (GAO) reported a dramatic increase in cyber attacks on federal agencies, as reported to the U.S. Computer Emergency Readiness Team (US-Cert). The cyber incidents totaled 41,776 in fiscal 2010, a 650 percent increase in five years.[144] During the month of August, there were 30 documented serious incidents of hacktivism. Hacktivism is defined as the use of computers and computer networks as a means of protest to promote political ends.[145] Some of the tools that are regularly used include Website defacements, redirects, denial-of-service attacks, information theft, Website parodies, virtual sit-ins, and virtual sabotage, all of which are crimes that would need to be investigated and prosecuted.

The specter of a potential attack, coupled with the increased incidents in hacking, have resulted in the creation of new policy and sections within DHS and DoD, in addition to the FBI, to prepare for, prevent, and mitigate attacks on the United States and its interests.[146] The DHS has been charged, by law, with certain cyber responsibilities; specifically "to protect the federal executive branch civilian agencies, and to lead the protection of critical cyberspace."[147] However, as with the intelligence community, there is a fragmented response to cyber issues as there is no one agency responsible for the entire over arching strategy.

In anticipation of potential attacks against U.S. interests in 2008, DHS created the National Cybersecurity Center (NCSC). The NCSC is tasked with protecting the government's cyber networks and will monitor, collect and share information regarding cyber security incidents on systems belonging to National Security Agency (NSA), FBI,

---

[143] Rollins and Henning, *Comprehensive National Cybersecurity Initiative*, 6.

[144] Behr, "A 'Smart' Grid Will Expose Utilities to Smart Computer Hackers."

[145] Samuel, "Hacktivism and the Future of Political Participation."

[146] White House, *International Strategy for Cyberspace*.

[147] Issac R. Porche, Jerry M. Sollinger, and Shawn McKay, *A Cyberworm that Knows no Boundaries* [occasional paper], (Santa Monica, CA: RAND, 2011), 27.

DoD, and DHS.[148] DHS Secretary Janet Napolitano reaffirmed the importance of this effort with the creation of a new National Cybersecurity and Communications Integration Center (NCCIC). In addition to its previous mission, it now includes "watch and warning" for incidents and threats that affect the nation's critical information technology and cyber infrastructure.[149]

In May of 2010, the DoD created the first U.S. Cyber Command and the first U.S. CYBERCOM Commander. These policies and agencies were implemented because of the increase in cyberattacks and threats against the military.[150] From these newly formed centers emerge national policies. In July 2011, DoD issued the *Department of Defense Strategy for Operating in Cyberspace*.[151] The White House has issued two policy papers, the *Comprehensive National Cybersecurity Initiative*[152] and the *International Strategy for Cyberspace*.[153]

The *Comprehensive National Cybersecurity Initiative* states that the President considers cyberspace to be of critical importance and appoints an executive branch Cyber security coordinator.[154] Additionally, it outlines 12 components for strengthening and addressing the federal networks as well as critical infrastructure. The 12 components address the key areas. If all areas could be addressed as easily as they are identified, it would greatly help the effort to strengthen the cyber risk. One of the key components identified directly pertains to this area of inquiry, specifically regarding supply chain threats. However, the weak link that is not addressed is the requirement that identifies which entity will have principal cyber security responsibility and does give one individual authority over all entities for cyber related efforts.

---

[148] Office of the Press Secretary, "Statement by Homeland Security Secreatary Michael Chertoff."

[149] Office of the Press Secretary, "Secretary Napolitano Opens New National Cybersecurity."

[150] Office of the Assistant Secretary of Defense, "DoD Anounces First U.S. Cyber Command."

[151] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace.*

[152] White House, *The Comprehensive National Cybersecurity Initiative.*

[153] White House, *International Strategy for Cyberspace.*

[154] White House, *The Comprehensive National Cybersecurity Initiative.*

The DoD *Strategy for Operating in Cyberspace* provided that the DoD create a new cyber command and a new cyber range testing ground for cyber security efforts to be tested and proven.[155] The policy stresses much of the information in the *National Cybersecurity Strategy*, emphasizing partnerships and the need for a secure and robust network (again covering the critical areas). The *International Strategy for Cyberspace* outlines and reiterates a little of both the *DoD Strategy* and the *National Cybersecurity Strategy*. It also addresses the critical nature of the Internet and the world dependence on it for global commerce and transnational connections. Furthermore, it advocates collaboration and partnerships on a worldwide scale to keep the Internet safe and secure, and global policing and prosecution of groups that perpetuate either disruption or interference with Internet traffic. It borrows from the *DoD Strategy for Operating in Cyberspace* and states, "[t]he United States has a compelling interest in defending its vital national assets, as well as our core principles and values, and we are committed to defending against those who would attempt to impede our ability to do so."[156] The issuance of these three policies, two of which emerged from the White House, captures the significance that the government has placed on cyberspace. A large amount of research and thought has been devoted to the core ideas of these strategies, but they are primarily focused around the federal network.

President Obama, via Presidential Directive, created the National Cyber Investigative Joint Task Force (NCIJTF) in 2008 to be the tip of the spear for a coordinated effort by all governmental agencies in domestic cyber investigations. This Task Force is represented by 18 intelligence and law enforcement agencies that have been charged with identifying key players and schemes. Its goal is to try to predict and prevent the developing trends in cybercrime or attacks and to pursue the persons behind the attacks.

Clearly, there are significant concerns surrounding this topic, so much so that the President has repeatedly made statements acknowledging the significance as to what is at stake. However, despite enactment of multiple policies, the introduction of several bills in

[155] White House, *International Strategy for Cyberspace.*

[156] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

Congress, and numerous Congressional hearings, little progress has been made toward a definitive plan for addressing the cyber issue. In fact, other than the previously discussed policies regarding the manufacture of microchips at a trusted foundry and the initiatives funded through DARPA/IARPA, there has been little other progress on the identification of compromised microchips. Other than a vague acknowledgement of a future policy on procurement, little of the recommendations in any of the numerous reports identified in this thesis have been implemented.

VII. CONCLUSION AND OPTIONS

According to government studies and findings by the private sector, China has engaged in numerous activities to exploit vulnerabilities found in technologies that support many U.S. financial and security processes. China is the number one threat to the United States with respect to cyber attacks and intellectual property theft, according to the findings published by the Office of National Counterintelligence Executive.[157] Colonel Jayson Spade says the People's Liberation Army (PLA) is preparing for total cyber warfare.[158] It is conducting cyberspace reconnaissance; creating the ability to do economic harm and damage critical infrastructure; preparing to disrupt communications and information systems necessary to support conventional armed conflict; and readying to conduct psychological operations to influence the will of the American people.[159] These attacks will exploit whatever vulnerabilities it has identified, including those that have been purposefully manufactured. There have been multiple instances of Chinese nationals infiltrating U.S. companies and later getting arrested for stealing intellectual property and designs,[160] and McAfee says China is the number one state-sanctioned hacking organization in the world. It is responsible for the majority of attacks against the U.S. government and the private industry.[161]

Much has been written on cyber security policy and how experts suggest best strategies to combat cyber attackers. These would include cyber terrorists and any other party that is a potential threat to the homeland. However I have been unable to find much documented information on the vulnerabilities of computer hardware. These vulnerabilities would be in the actual components themselves.

---

[157] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyber Space* (Washington, D.C.: Office of the National Counterintelligence Executive, 2011).

[158] Jason M. Spade, *Information as Power: China's Cyber Power and America's National Security* (Carlisle Barracks, PA: U.S. Army War College, 2012).

[159] Spade, *Information as Power*.

[160] Riley and Vance, "It's Not Paranoia if They're Stealing Your Secrets."

[161] Michael Kan, "China's Top Paper Dismisses McAfee Hacking Report," *Computerworld*, August 5, 2011.

One of the articles I have found is "Old Trick Threatens the Newest Weapons,"[162] wherein Markoff talks about the potential threat of creating computer chips and hardware that has vulnerabilities built into it at the time of manufacture. He implies that 98 percent of all computer hardware is purchased and built outside of the United States and its sterility cannot be validated.[163] This concern has prompted the NSA to create its own manufacturing plant for the most sensitive equipment, but that amounts to less than two percent of the computers the government procures. Markoff suggests that hardware can be in effect a Trojan horse wherein it is procured and deployed, and when the moment is right, vulnerability is exploited or other attack is initiated.[164] The concern is that the compromised hardware can never be identified and acts as a sleeper until either it is signaled or the requisite time has passes for its job to be preformed. John Villasenor, of UCLA, says "…the need to proactively address hardware security remains widely underappreciated"[165] when speaking about the importance of ensuring hardware security in the age of globalization and the complex issues that accompany it.

The discovery by Sergei Skorobogatov of Cambridge University validates the concerns that have been sounded by many previously.[166] This is the first documented incident of purposefully manufactured hardware vulnerability. The implications to the homeland security enterprise are enormous. The fact that there is an identified security flaw in a microchip that potentially is used in military, government, and other critical infrastructure, regardless of how it was implemented, must be addressed quickly to ensure that it is not exploited by either those who put it there or other malicious actors. It is specifically in this area that more research needs to be completed. There is very little research available and, although acknowledged as a significant threat, the security concerns about microchips are not adequately addressed in policy or other documents.

---

[162] Markoff. "Old Trick Threatens the Newest Weapons."

[163] Ibid.

[164] Ibid.

[165] Villasenor, "Ensuring Hardware Cybersecurity."

[166] Skorobogatov and Woods, *Breakthrough Silicon Scanning*.

What can be done to address the vulnerability? First and foremost, acknowledge there is an issue and take action rather than deny that there is a problem.[167] All microchips that are brought into the U.S. for use in critical systems must be randomly checked for vulnerability. The feasibility for complete testing on every microchip is not viable due to time and cost factors. Appropriate action needs to be taken for any identified offending manufacturers. This would be a potential political issue if it was determined that a nation state was involved. A full investigation would be required for any U.S. based company involvement to determine the extent of the company's knowledge and/or collusion, which would then have to be addressed as well. A strategy must be developed that prioritizes, based on criticality, the replacement of the compromised hardware from trusted manufacturers' products. This may require sections of industry, government or infrastructure to be operating at a less than optimal level during the remediation.

For the future, clear legislation must be enacted, defining not only the cyber parameters but also the boundaries or jurisdictional lines. The federal government is currently the responsible party for investigation of cyber crimes; however the number of incidents reported continues to grow at an almost exponential level. This will require a push down to the local level for some of these investigations, which can only be accomplished through legislation. In addition policy needs to be created clearly delineating the hierarchy for cyber activities. A single responsible person with appropriate authority needs to coordinate all cyber activities. Responsibilities can be delegated to agencies based on expertise, but a repeat of what has occurred with intelligence cannot be allowed to happen again.

There is extensive writing concerning cyber security. Most of this writing is related to malware and software attacks. There is little written with respect the hardware itself, which may be the largest vulnerability. As explained above, the concept of cyber security as it relates to hardware is almost non-existent. There are many hardware

[167] Aliya Sternstein, "Defense Rejects Rigid Supply Chain Security Countermeasures," *Nextgov*, September 27, 2012, http://www.nextgov.com/cybersecurity/2012/09/defense-rejects-rigid-supply-chain-security-countermeasures/58408/ (accessed October 23, 2012).

vectors that can be exploited to produce vulnerabilities. The security phenomenon for hardware has only recently begun to be exposed and documented. Most of the literature describes a potential risk or outlines some possible threats, but specific documented incidents there is little information available.

There has been a great deal of interest, study, and reporting on hardware and recently the security implications. While there is a well-developed understanding on the topic, our understanding of current vulnerability for homeland security would be improved by further research on what the vulnerabilities are and how we can mitigate that threat. Identifying how we can prevent these issues or at least understand them will allow decision makers and agencies involved to learn more about this important topic. The DoD has recognized the potential significance of this issue and initiated a supply chain risk management (SCRM) policy to address the vulnerabilities, with an implementation target date of FY2016.[168] However, in the same breath, they say:

…outdated constructs of a static or stale industrial base, where the U.S. government could dictate certain assurances or impose inflexible rules on our suppliers, must give way to the facts on the ground that our base is no longer a single monolithic entity. Any industrial base supply chain policy must take these facts into account."[169]

This statement almost negates any action to address the supply chain issue. This is the only actual strategy that has been targeted for implementation amongst all of the many that have been offered in the multitude of reports on these issues. It is therefore recommended that the suggestions proposed in the 2005 *High Performance Microchip Supply* report coupled with the suggestions in the newer 2010 *Security Risk Management for the Off-the Shelf (OTS) Information and Communications Technology (ICT) Supply Chain* report be implemented to create an overarching microchip supply chain policy. This will afford the best possible solution to combat the vulnerabilities in the microchip supply chain. This will also allow collaboration within the DHS as well as between other

[168] Krekel, Adams and Bakos, *Occupying the Information High Ground*.

[169] Sternsetin, "Defense Rejects Rigid Supply Chain Security Countermeasures."

agencies and nations. With the latest in technological advances, it will not only optimize the ability of our personnel, but also enhance the overall effectiveness of the government.

I would like to close with the thought that the issues surrounding cyber security are similar in nature to those we in police work face routinely. Conventional crimes, such as robbery or burglary occur routinely and have never been eliminated despite employing a myriad of strategies such as alarm systems and locks or even deterrence via laws and penalties. Instead policing service and investigations have to be provided to arrest the perpetrators and take them off the street. This is what impacts criminals and brings down the crime rate. What we have already addressed in policing though is the defined boundaries or jurisdictions. The defining of boundaries will prove to be the key to successful cyber security. If not, then we may face a "cyber Pearl Harbor" as Secretary of Defense Leon Panetta warned.[170] Or as General Keith B. Alexander, commander of .U.S Cyber Command and director of the National Security Agency (NSA) succinctly said, the U.S. is facing '"death by a thousand cuts" in cyberspace.[171]

[170] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.

[171] Dan Verton, "Cybersecurity: US Facing 'Death by a Thousand Cuts' in Cyberspace," October i8, 2012, http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-thousand-cuts-in-cyberspace.html (accessed October 23, 2012).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. SIGNIFICANT CYBER INCIDENTS SINCE 2006 AS PER THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES[172]

This list is a work in progress that we update as new incidents come to light. If you have suggestions for additions, send them to techpolicy@csis.org. Significance is in the eye of the beholder, but we focus on successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

1. ***May 2006***. The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards, and spend the night carting off file cabinets it would be an act of war, but when it happens in cyberspace we barely notice.

2. ***August 2006***. A senior Air Force Officer stated publicly, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (the unclassified military network)."

3. ***November 2006***. Hackers attempted to penetrate U.S. military War College networks, resulting in a two week shutdown at one institution while infected machines are restored.

4. ***December 2006***. NASA was forced to block emails with attachments before shuttle launches out of fear that they would be hacked. *Business Week* reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.

5. ***2006.*** Chinese hackers were thought to be responsible for shutting down the House of Commons computer system.

6. ***April 2007***. The Department of Commerce had to take the Bureau of Industrial Security's networks offline for several months because its networks were hacked by

[172] Lewis, *Significant Cyber Events Since 2006*.

unknown foreign intruders. This Commerce Bureau reviews confidential information on high tech exports.

7. ***May 2007***. The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.

8. ***May 2007***. Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well; however, the attacks created a wave of fear in cyber dependent countries like the U.S.

9. ***June 2007***. The Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit DoD networks.

10. ***August 2007***. The British Security Service, the French Prime Minister's Office, and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

11. ***September 2007***. Israel disrupted Syrian air defense networks (with some collateral Damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility.

12. ***September 2007***. Francis Delon, Secretary-General of National Defence in France, stated that information systems in France had been infiltrated by groups from China.

13. ***September 2007***. Contractors employed by DHS and DoD had their networks hacked as backdoors into agency systems.

14. ***September 2007***. British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments.

15. ***October 2007***. China's Ministry of State Security said that foreign hackers, 42 percent from Taiwan and 25 percent from United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

16. ***October 2007***. More than a thousand staffers at Oak Ridge National Labs received an email with an attachment that, when opened, provides unknown outsiders with access to the lab's databases.

17. ***November 2007***. Jonathan Evans, the head of Britain's Security Service (MI5), warned 300 business firms of the increased online threat from Russian and Chinese state organizations saying, "A number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They…increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks."

18. ***January 2008***. A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.

19. ***March 2008***. South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.

20. ***March 2008***. U.S. officials reported that American, European, and Japanese companies were experiencing significant losses of intellectual property and business information to criminal and industrial espionage in cyberspace; however, details cannot be provided in an unclassified setting.

21. ***April – October 2008***. A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated

from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department.

22. ***May 2008***. The *Times of India* reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict.

23. ***June 2008***. The networks of several Congressional offices were hacked by unknown foreign intruders. Some infiltrations involved offices with an interest in human rights in Tibet.

24. ***Summer 2008***. The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

25. ***Summer 2008***. Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data detailing the quantity, value, and location of oil discoveries around the world. One company put the losses in the millions.

26. ***August 2008***. Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government Websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions.

27. ***October 2008***. Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

28. ***November 2008***. Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million dollars from machines in 49 cities.

29. ***November 2008***. Classified networks at DoD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and re-secure the networks.

30. ***December 2008***. Retail giant TJX was hacked. The one hacker captured and convicted (Maksym Yastremskiy) is said to have made $11 million from the hack.

31. ***December 2008***. Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some CSIS staff would go into the new administration and may have though it might be interesting to read their emails beforehand.

32. ***2008***. Britain's MPs were warned about e-mails apparently sent by the European Parliament amid fears that they could be used by Chinese hackers to implant viruses.

33. ***January 2009***. Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government Websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.

34. ***January 2009***. Indian Home Ministry officials warned that Pakistani hackers had placed malware on popular music download sites used by Indians in preparation for cyber attacks.

35. ***February 2009***. FAA computer systems were hacked. Increased use by FAA of IP-bases' networks also increases the risk of the intentional disruption of commercial air traffic.

36. ***February 2009***. 600 computers at India's Ministry of External Affairs were hacked.

37. ***February 2009***. French naval aircraft planes were grounded after military databases were infected with the "confickr" virus. Naval officials suspected someone at the Navy had used an infected USB key.

38. ***March 2009***. The German government warned that hackers were offering a free version of the new Microsoft operating system that installs Trojans.

39. ***March 2009***. Canadian researchers found a computer espionage system that they believe China implanted on the government networks of 103 countries.

40. ***March 2009***. Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

41. ***April 2009***. *Wall Street Journal* articles laid out the increasing vulnerability of the U.S. power grid to cyber attack also highlighted was the intrusions into F-35 databases by unknown foreign intruders.

42. ***April 2009***. Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National People's Congress.

43. ***April 2009***. Chinese hackers reportedly infiltrated South Korea's Finance Ministry via a virus attached to e-mails claiming to be from trusted individuals.

44. ***May 2009***. In May 2009, Merrick Bank, a leading issuer of credit cards, claimed it lost $16 million after hackers compromised as many as 40 million credit card accounts.

45. ***May 2009***. The Homeland Security Information Network (HSIN) was hacked by unknown intruders. The hackers gained access to the data by getting into the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed

46. ***June 2009***. The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated.

47. ***June 2009***. German Interior Minister Wolfgang Schaeuble noted, when presenting the Interior Ministry's 2008 security report, that China and Russia were increasing espionage efforts and Internet attacks on German companies.

48. ***July 2009***. Cyberattacks against Websites in the United States and South Korea, including a number of government Websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention.

49. ***August 2009***. Albert Gonzalez was indicted on charges that between 2006 and 2008, he and unidentified Russian or Ukrainian colleagues allegedly stole more than 130 million credit and debit cards by hacking into the computer systems of five major companies. This was the largest hacking and identity theft crime in U.S. history.

50. ***August 2009***. Ehud Tenenbaum was convicted of stealing $10 million from U.S. banks. Tenenbaum was known for hacking into DoD computers in 1998, which resulted in a sentence of six months of community service from an Israeli court.

51. ***November 2009***. Jean-Pascal van Ypersele, the vice-chairman of the United Nations' Intergovernmental Panel on Climate Change, ascribed the hacking and release of thousands of emails from the University of East Anglia's Climatic Research Unit to Russia as part of a plot to undermine the Copenhagen climate talks.

52. ***December 2009***. The *Wall Street Journal* reported that a major U.S. bank had been is hacked, losing tens of millions of dollars.

53. ***December 2009***. Downlinks from U.S military UAV's were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV has viewed.

54. ***January 2010***. The UK's MI5 Security Service warned that undercover intelligence officers from the People's Liberation Army and the Ministry of Public Security have approached UK businessmen at trade fairs and exhibitions with the offer of "gifts" - cameras and memory sticks - which contain malware that provides the Chinese with remote access to users' computers.

55. ***January 2010***. Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other U.S. companies. The goal of

the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

56. ***January 2010***. Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers in December 2009, according to leaked e-mails from a cyber-security company working for the bank.

57. ***January 2010***. M. K. Narayanan, India's National Security Adviser, said his office and other government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to penetrate Indian government computers.

58. ***January 2010***. A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December and with a similar message.

59. ***January 2010***. Intel disclosed that it has experienced a cyber attack at about the same time that Google, Adobe, and other were attacked. The hackers exploited the vulnerabilities in Internet Explorer software that had been used in the other attacks as well. Intel said that there was no intellectual property or financial loss.

60. ***March 2010***. NATO and the EU warned that the number of cyber attacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

61. ***March 2010***. Google announced that it had found malware targeted at Vietnamese computer users. Google said that the malware was not especially sophisticated and was used to spy on "potentially tens of thousands of users who downloaded Vietnamese keyboard language software" the malware also launched distributed denial of service attacks against blogs containing political dissent, specifically, opposition to bauxite mining efforts in Vietnam.

62. ***March 2010.*** Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China, to gain inside information on the trial defense strategy.

63. ***March 2010***. Unknown hackers post the real incomes of Latvian government officials after accessing their tax records, creating political turmoil.

64. ***April 2010***. Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems.

65. ***April 2010***. A Chinese telecommunications firm accidently transmitted erroneous routing information for roughly 37,000 networks, causing internet traffic to be misrouted through China. The incident lasted 20 minutes and exposed traffic from more than 8,000 U.S. networks, 8,500 Chinese networks, 1,100 Australian networks, and 230 French networks.

66. ***May 2010***. A leaked memo from the Canadian Security and Intelligence Service (CSIS) says "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

67. ***July 2010***. A Russian intelligence agent (allegedly named Alexey Karetnikov), was arrested and deported after working for nine months as a software tester at Microsoft.

68. ***October 2010***. Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

69. ***October 2010***. The *Wall Street Journal* reported that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over

$12 million from five banks in the U.S. and UK. Zeus uses links in emails to steal account information, which the hackers then use to transfer money into bank accounts they control. 100 “mules”, or low end criminals, were arrested for opening bank accounts under false names into which the hackers transferred stolen money.

70. ***October 2010***. Australia’s Defence Signals Directorate reported a huge increase in cyberattacks on the military. Australia’s Defence Minister, John Faulkner, revealed there had been 2400 “electronic security incidents” on Defence networks in 2009 and 5551 incidents between January and August 2010.

71. ***December 2010***. British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defence contractor and other “British interests” that evaded defenses by pretending to come from the White House.

72. ***December 2010***. India’s Central Bureau of Investigation (CBI) Website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected.

73. ***January 2011***. Hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and stole more than $7 million in credits, forcing the market to shut down temporarily.

74. ***January 2011***. Hacker extracted $6.7 million from South Africa's Postbank over the New Year's Holiday.

75. ***January 2011***. The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada’s main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.

76. ***March 2011***. Hackers penetrated French government computer networks in search of sensitive information on upcoming G-20 meetings.

77. ***March-April 2011***. Between March 2010 and April 2011, the FBI identified 20 incidents in which the online banking credentials of small-to-medium sized U.S.

businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

78. ***March-April 2011***. Hackers used phishing techniques in attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

79. ***April 2011***. Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

80. ***April 2011***. Employees at Oak Ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007.

81. ***May 2011***. Cybercriminals masquerading as member of the hacktivist group "Anonymous" penetrated the PlayStation network. Sony estimated that personal information for more than 80 million users was compromised and that the cost of the breach at over $170 million.

82. ***June 2011***. The IMF's networks were compromised reportedly by a foreign government using fraudulent emails with malware attachments, and a "large quantity of data, including documents and e-mails," are exfiltrated.

83. ***June 2011***. Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

84. ***July 2011***. In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen.

85. ***July 2011***. The German Bundespolizei (Federal Police) and the Bundeszollverwaltung (Federal Customs Service) discovered that servers used to locate serious criminals and terrorism suspects by gathering information from GPS systems in

cars and mobile phones were penetrated (using a phishing attack)as early as 2010. Following the cyberattack, the relevant servers had to be temporarily shut down to prevent further data losses.

86. ***July 2011***. South Korea said hackers from China had penetrated an internet portal and accessed phone numbers, e-mail addresses, names, and other data for 35 million Koreans.

87. ***August 2011***. According to sources in the Japanese government, Mitsubishi Heavy Industries and 20 other Japanese defense and high tech firms were the target of an effort to extract classified defense information. Japanese officials believed the exploits all originated from the same source. The intruder used email with a malicious attachment whose contents were the same as a legitimate message sent 10 hours earlier.

88. ***August 2011***. Email and documents from 480 members of the Japanese Diet and lawmakers and their staff were compromised for a month after a phishing attack implanted a Trojan on members' computers and Diet servers. The hijacked machines communicated with a server in China and the attackers included Chinese characters in their code.

89. ***September 2011***. Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates are used to verify that a Website is genuine. By issuing a false certificate, an attacker can pretend to be a secure Website, intercept e-mail, or install malicious software. This was the second hack of a certificate authority in 2011.

90. ***September 2011***. Australia's Defense Signals Directorate says that defense networks are attacked more than 30 times a day, with the number of attacks increasing by more than 350 percent by 2009.

91. ***September 2011***. A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for U.S. Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The U.S. did not lose control of any drone nor does it appear

that any data was exfiltrated, but the malware was persistent and took several attempts to remove.

92. ***October 2011***. Networks of 48 companies in the chemical, defense, and other industries were penetrated for at least six months by a hacker looking for intellectual property. Symantec attributes some of the attacks to computers in Hebei, China.

93. ***November 2011***. Norway's National Security Agency (NSM) reports that at least 10 major Norwegian defense and energy companies were hacked. The attacks were specifically "tailored" for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords.

94. ***December 2011***. U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the People Liberation Army. The hackers had access to access to everything in Chamber computers, including member company communications and industry positions on U.S. trade policy.

95. ***March 2012***. NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

96. ***March 2012.*** The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC's Director General blamed Iran for the incident.

97. ***March 2012***. India's Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government Websites had been compromised from December 2011 to February 2012. Most of the

incidents involved Website defacement and many of the hacks appeared to originate in Pakistan.

98. ***March 2012***. The U.S. Department of Homeland Security issued amber alerts warning of a cyber intrusion campaign on U.S. gas pipelines, dating back to December 2011. Press reports indicated that Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) described the attack as a sophisticated spear phishing campaign emanating from a single source.

99. ***May 2012***. UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks.

100. May 2012. An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world.

101. ***May 2012***. Researchers at the University of Toronto report that versions of the installer for the proxy tool Simurgh, which anonymizes net use and is popular in countries such as Iran and Syria to circumvent government internet controls, also installs a keylogger Trojan which sends the user name, keystrokes, and program use to another site.

102. ***June 2012***. A phishing campaign targets the U.S. aerospace industry experts attending the 2013 IEEE Aerospace Conference.

103. ***June 2012***. A global fraud campaign using automated versions of SpyEye and Zeus Trojans targeted high-value personal and corporate accounts and bypassed two-factor authentication.

104. ***June 2012***. The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of state cyber attacks.

105. ***July 2012***. A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings.

106. ***July 2012***. Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems.

107. ***July 2012***. The Director of the National Security Agency said that there had been a 17-fold increase in cyber incident at American infrastructure companies between 2009 and 2011.

108. ***August 2012***. Malware nicknamed "Gauss," infected 2,500 systems worldwide. Gauss appears to have been aimed at Lebanese banks, and contains code whose encryption has not yet been broken.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. GLOSSARY OF TERMS

Authorization—A right or a permission that is granted to a system entity to access a system resource.

Backdoor—A hidden method for bypassing normal computer authentication.

BIOS—Basic Input/Output System or Basic Integrated Operating System. BIOS refers to the software code run by a computer when first powered on. The primary function of BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer. This process is known as booting up.

Control System (CS)—An interconnection of components (computers, sensors, actuators, communication pathways, etc.) connected or related in such a manner to command, direct, or regulate itself or another system, such as chemical process plant equipment/system, oil refinery equipment/systems, electric generation/

Encryption—In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge.

Firmware—Software that is embedded in a hardware device. It is often provided on flash ROMs or as a binary image file that can be uploaded onto existing hardware by a user.

Malware—Malicious software designed to infiltrate or damage a computer system, without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, Root kits, spyware, and adware.

Network Device—A computer connected to a network providing services to and/or using services from other network devices. Also called a network node.

Packet—A structured and defined part of a message transmitted over a network.

Patch—A fix for a software program where the actual binary executable and related files are modified.

Programmable Logic Controller (PLC)—A programmable microprocessor-based device designed to control and monitor various inputs and outputs used to automate industrial processes.

Port—Hardware Port: An outlet on a piece of equipment into which a plug or cable connects. Network port: An interface for communicating with a computer program over a network. I/O or machine port - port-mapped I/O: Nearly all processor families use the same assembly instructions for memory access and hardware I/O. Software port: Software is sometimes written for specific processors, operating systems, or programming interfaces. A software port is software that has been changed to work on another system.

Root kits—Sets of programs that are introduced into a computer system without permission of the computer operator to obtain privileged access, which would allow control of the computer, usually with capabilities to avoid detection.

Supervisory Control and Data Acquisition (SCADA)—A SCADA computer system is developed for gathering and analyzing real time data. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water and waste control, energy, oil and gas refining, and transportation.

Server—A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files, a Web server for access to Web content, a DNS server for domain name services, a database server for access to relational tables, an e-mail server for access to e-mail, etc.

Services—Software application that facilitates communications to other applications or devices either local or distributed. Services are typically associated to a port. Sometimes services are referred to as software ports.

Upgrade—Generally, an upgrade is a new release of software, hardware, and/or firmware replacing the original components to fix errors and/or vulnerabilities in software and/or provide additional functionality and/or improve performance.

Validate—To give evidence for or establish the soundness of. Validation is a process of checking documents or testing against a formal standard.

Virus—Software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs. See Malware.

Worm—A computer worm is a self-replicating computer program similar to a computer virus. In general, worms harm the network and consume bandwidth.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"2011 Major Integrated Circuit Foundries" [Strategic Reviews Database, company reports]. *IC Insights*. 2011.

Abel, David M. and Kyle I. Fox. *Sleeper Cells in Cyberspace: Analyzing Supply Chain Malware Incidents for Offensive and Defensive Implications*. Master's thesis, Naval Postgraduate School, 2011.

"Actel Leverages UMC Foundry Solutions for 65nm eFlash FPGAs." *Design and Reuse News*. November 18, 2008. http://www.design-reuse.com/news/19553/65nm-eflash-fpga.html. Accessed November 8, 2012.

"Actel ProASIC3/E Production FPGAs, Features and Advantages." Microsemi SoC Products Group. 2007. http://www.actel.com/documents/PA3E Tech WP.pdf. Accessed October 21, 2012.

Adee, Sally. "The Hunt for the Kill Switch." *Spectrum, IEEE* 45, no. 5 (2008).

Barboza, David, Peter Lattman, and Catherine Rampell. "How the U.S. Lost Out on iPhone Work." *New York Times*. January 21, 2012.

Behr, Peter. "A 'Smart' Grid Will Expose Utilities to Smart Computer Hackers." *New York Times*. April 19, 2011.

Bumiller, Elisabeth and Thom Shanker. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*. October 11, 2012.

Carlson, Gwen. "Actel Expands Military-Qualified Flash-Based FPGA Offerings" [press release]. Microsemi Soc Products Group. August 11, 2008. http://www.actel.com/company/press/2008/8/11/. Accessed November 8, 2012.

Defense Science Board. *High Performance Microchip Supply*. Washington, D.C.: Department of Defense, 2005.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington, D.C.: Department of Defense, 2011.

Derene, Glenn and Joe Pappalardo. "Counterfeit Chips Raise Big Hacking, Terror Threats, Experts Say." *Popular Mechanics Online*. October 2009. http://www.popularmechanics.com/technology/gadgets/news/4253628. Accessed July 10, 2012.

"Editor." Webster's Online Dictionary. http://www.websters-online-dictionary.org/definitions/pwn. Accessed October 22, 2012.

Federal Business Opportunities. "DARPA." https://www.fbo.gov/?s=opportunity&mode=form&id=406db188e0e1935a806c143a5603eb48&tab=core&_cview=0. Accessed January 28, 2012.

Federal Business Opportunities. "Integrity and Reliability of Integrated Circuits (IRIS)." https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=30191c1ba1db9c257723e48b97d4c155&_cview=0. Accessed January 28, 2012.

French, Michael. *US Economic History since 1945*. New York: Manchester University Press, 1997.

Georgia Tech University. *Emerging Cyber Threats Report 2012*. Atlanta, GA: Georgia Tech University, 2011.

Government Accounting Office. *IT Supply Chain National Security: Related Agencies Need to Better Address Risks*. Washington, D.C.: United States Government Accountability Office, 2012.

———. *Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India*. Washington, DC: Government Accounting Office, 2006.

Gwon, Youngjune L., H. T. Kung, and Dario Vlah. "DISTROY: Detecting Integrated Circuit Trojans with Compressive Measurements." *6th USENIX Workshop on Hot Topics in Security (HotSec)* 36, no. 6 (December 2011).

Harada, Lawrence K. *Semiconductor Technology and U.S. National Security*. Carisle, PA: U.S. Army War College, 2010.

Hutton Wade, Alexander, C. David Hylendar, Joseph Pamula, Christopher Porter, and Marc Spitler Baker. *2011 Data Breech Investigations Report*. New York: Verizon, 2011.

"The Integrated Circuit." May 5, 2003. http://www.nobelprize.org/educational/physics/integrated_circuit/history/. Accessed October 22, 2012.

"Intel." Intel Corporation. http://www.intel.com/content/www/us/en/homepage.html#. Accessed November 8, 2012.

International Directory of Company Histories. s.v. "Intel Inc." 2002. http://www.encyclopedia.com/topic/Intel_Corp.aspx. Accessed November 8, 2012.

Jackson Higgins, Kelly. “Sykipot Malware Now Steals Smart-Card Credentials.” *Information Week Online*. January 12, 2012. http://www.darkreading.com/authentication/167901072/security/attacks-breaches/232400288/sykipot-malware-now-steals-smart-card-credentials.html. Accessed October 22, 2012

Johnson, Bryan T. “The Heritage Foundation Research: Asia.” The Heritage Foundation, January 24, 1991. http://www.heritage.org/research/reports/1991/01/bg805-the-us-japan-semiconductor-agreement. Accessed November 8, 2012.

Kan, Michael. “China’s Top Paper Dismisses McAfee Hacking Report.” *Computerworld*. August 5, 2011.

Keizer, Gregg. “Best Buy Sold Infected Digital Picture Frames.” *Computerworld Online*. January 23, 2008. http://www.computerworld.com/s/article/9058638/Best_Buy_sold_infected_digital_picture_frames. Accessed October 10, 2012.

Krekel, Bryan, Patton Adams, and George Bakos. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington, D.C.: Northrop Grumman Corp., 2012.

LaFraniere, Sharon. “Facing Counterfeiting Crackdown, Beijing Vendors Fight Back.” *New York Times*. March 1, 2009.

Lewis, James Andrew. *Significant Cyber Events since 2006*. Washington, D.C.: Center for Strategic and International Studies, 2012.

Madsen, Marcia G., Louis M. Addeo, Frank J. Anderson, Jr., Dr. Allan V. Burman, Carl DeMaio, Marshall J. Doke, Jr., David A. Drabkin, Jonathan L. Etherton, James A. Hughes, Deidre A. Lee, Tom Luedtke, Joshua I. Schwartz, and Roger D. Waldron. *Report of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress*. Washington, D.C.: Congressional Budget Office, 2007.

Markoff, John. “Old Trick Threatens the Newest Weapons.” October 27, 2009. *The New York Times*. http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all. Accessed November 20, 2011.

Martin, Jonathan, David Salamie, Nelson Rhodes, “National Semiconductor Corporation.” *International Directory of Company Histories*. 2005, http://www.encyclopedia.com/doc/1G2-3429600082.html. Accessed November 8, 2012.

Maxfield, Clive. *The Design Warrior's Guide to FPGAs*. Burlington, MA: Elsevier, 2004

McCormack, Richard. "$600 Million Over 10 Years for IBM's 'Trusted Foundry' Chip Industry's Shift Overseas Elicits National Security Agency, Defense Department Response." *Manufacturing and Technology News*. February 3, 2004. http://www.manufacturingnews.com/news/04/0203/art1.html. Accessed October 23, 2012.

Michaels, Spencer. *The Growth of the Microchip* [PBS interview by Jim Lehrer online]. January 1, 1993. *PBS Newshour*. http://www.pbs.org/newshour/bb/business/jan-june93/chip_1-1-93.html. Accessed October 1, 2012.

Microsemi SoC Products Group. *Microsemi SoC Products Group—Partners*. 2012. http://www.actel.com/products/partners/solution/ip/specialization.aspx. Accessed November 8, 2012.

Mosteller, Kristy, Holly McKinley Schmidt, Stephanie Shankles, and Theodore Winograd Karen Goertzel. *Security Risk Management for the Off-the Shelf (OTS) Information and Communications Technology (ICT) Supply Chain*. Herndon, VA: Information Assurance Technology Analysis Center, 2010.

Oates, John. "Biting the Hand that Feed IT." *The Register*. July 21, 2010.

———. "Dell Warns on Spyware Infected Server Motherboards." *The Register Online*. July 21, 2010. http://www.theregister.co.uk/2010/07/21/dell_server_warning/. Accessed September 20, 2012.

Office of the Assistant Secretary of Defense (Public Affairs). "DoD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander" [press release]. May 21, 2010. http://www.defense.gov/Releases/Release.aspx?ReleaseID=13551. Accessed August 18, 2011.

Office of Management and Budget. "IT Dashboard." August 31, 2012. http://www.itdashboard.gov/portfolios. Accessed October 22, 2012.

Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyber Space*. Washington, D.C.: Office of the National Counterintelligence Executive, 2011.

Office of the Press Secretary. "Secretary Napolitano Opens New National Cybersecurity and Communications Integration Center" [press release]. October 30, 2009. http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm. Accessed August 18, 2011.

———. “Statement by Homeland Security Secretary Michael Chertoff on the Appointment of the Director of the National Cyber Security Center” [press release]. March 20, 2008. http://www.dhs.gov/xnews/releases/pr_1206047924712.shtm. Accessed August 18, 2011.

Office of the Under Secretary of Defense Acquisition (Technology & Logistics). *Special Technology Area Review on Field Programmable Gate Arrays (FPGAs) for Military Applications*. Washington, D.C.: Department of Defense Advisory Group on Electron Devices, 2005.

Porche, Issac R., Jerry M. Sollinger and Shawn McKay. *A Cyberworm that Knows no Boundaries* [occasional paper]. Santa Monica, CA: RAND, 2011.

President’s Blue Ribbon Commission on Defense Management [The Packard Commission]. *A Quest for Excellence: Final Report to the President and Appendix, Final*. Washington, D.C.: Packard Commission, 1986.

Rawnsley, Adam. “Can Darpa Fix the Cybersecurity ‘Problem From Hell?’” *Wired*, August 5, 2011.

Riley, Michael and Ashlee Vance. “Cyber Weapons: The New Arms Race.” *Bloomberg Business Week*. July 20, 2011.

———. “It’s Not Paranoia if They’re Stealing Your Secrets.” *Bloomberg Business Week*. March 19, 2012.

Rogers, Mike and Charles Albert Ruppersberger. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Washington, D.C.: House of Representatives, 2012.

Rollins, John and Anna C. Henning. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*. Washington, D.C.: Congressional Research Service, 2011.

Samuel, Alexandra. “Hacktivism and the Future of Political Participation.” August 2004. http://www.alexandrasamuel.com/dissertation/index.html. Accessed July 15, 2012.

Skorobogatov, Sergei and Christopher Woods. *Breakthrough Silicon Scanning Discovers Backdoor in Military Chip*. Cambridge, MA: Cambridge University, 2011.

Spade, Jason M. *Information as Power: China’s Cyber Power and America's National Security*. Carlisle Barracks, PA: U.S. Army War College, 2012.

Sternstein, Aliya. “Defense Rejects Rigid Supply Chain Security Countermeasures.” *Nextgov*. September 27, 2012. http://www.nextgov.com/cybersecurity/2012/09/defense-rejects-rigid-supply-chain-security-countermeasures/58408/. Accessed October 23, 2012.

Symantec. *Norton Study Calculates Cost of Global Cybercrime: $114 Billion Annually*. Mountain View, CA: Symantec, 2011.

Techterms Computer Dictionary. s.v. “cybercrimes.” http://www.techterms.com/definition/cybercrime. Accessed September 22, 2011.

Techterms Computer Dictionary. s.v., “integrated circuit.” http://www.techterms.com/definition/integratedcircuit. Accessed November 8, 2012.

“Texas Instruments Inc.” *International Directory of Company Histories*. 2002. http://www.encyclopedia.com/doc/1G2-2845000111.html. Accessed October 23, 2012.

Tucek, Joseph, Anthony Cozzie, Chris Grier, Weihang Jiang, Yuanyuan Zhou, and Samuel T. King. *Designing and Implementing Malicious Hardware*. Urbana, IL: USENIX Association, 2008.

Ungerleider, Neal. “DHS: Imported Consumer Tech Contains Hidden Hacker Attack Tools.” *Fast Company*. July 7, 2011. http://www.fastcompany.com/1765855/dhs-imported-consumer-tech-contains-hidden-hacker-attack-tools. Accessed October 10, 2012.

“U.S.-based Companies Held 12 of the Top 25 Fabless Spots in 2011.” IC Insights. 2011. http://www.icinsights.com/news/bulletins/USbased-Companies-Held-12-Of-The-Top-25-Fabless-Spots-In-2011/. Accessed October 23, 2012.

Vargo, Mike. “Innovation in an Offshoring Economy.” *CIT Engineering Magazine*, winter 2011.

Verton, Dan. “Cybersecurity: US Facing ‘Death by a Thousand Cuts’ in Cyberspace.” October i8, 2012. http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-thousand-cuts-in-cyberspace.html. Accessed October 23, 2012.

Villasenor, John D. “Ensuring Hardware Cybersecurity.” *Issues in Technology Innovation*, no. 9 (May 2011).

———. “The Hacker in Your Hardware.” *Scientific American* 303, no. 2 (2010): 82–88.

White House. *The Comprehensive National Cybersecurity Initiative*. Washington, D.C.: White House, 2008.

———. *Cyber Space Policy Review*. Washington, D.C.: White House, 2009.

———. *International Strategy for Cyberspace Prosperity, Security, and Openness in a Networked World*. Washington, D.C.: White House, 2011.

Wilson, Tim. "State of Security: What Keeps Infosec Pros Awake at Night?" *Information Week*. February 2009.

Wong, William. "Electronic Design." September 7, 2006. http://electronicdesign.com/article/embedded/eied-online-fpga-3-actel-proasic-starter-kit13423. Accessed October 8, 2012.

Zetter, Kim. "Meet 'Flame,' the Massive Spy Malware Infiltrating Iranian Computers." *Wired Magazine*. May 12, 2012.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California