Global Innovation and Strategy Center

US Reliance on Foreign IT

Mitigating Risks Associated with Foreign Sources of Hardware Components

Summer 2008 – Project 08-03
August 2008

Intern Researchers:

Amanda Jokerst
James Martin
Kristen Rodgers
Keith Roland
Erica Tesla

Project Management and Oversight:

1Lt Kevin Johnson
John G. Hudson II
Stephanie Silva

Approved: Kevin E. Williams, SES, DAF
Director, Global Innovation and Strategy Center

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
OCT 2008	FINAL REPORT	MAY 2008 - AUGUST 2008

4. TITLE AND SUBTITLE

U.S. Reliance on Foreign IT: Mitigating Risks Associated with Foreign Sources of Hardware Components

5a. CONTRACT NUMBER

N/A

5b. GRANT NUMBER

N/A

5c. PROGRAM ELEMENT NUMBER

N/A

6. AUTHOR(S)

Jokerst, Amanda
Martin, James
Rodgers, Kristen
Roland, Keith
Tesla, Erica

5d. PROJECT NUMBER

08-03

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
Intern Program
6805 Pine Street
Omaha, NE 68106

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

USSTRATCOM Global Innovation and Strategy Center (GISC)
6805 Pine Street
Omaha, NE 68106

10. SPONSOR/MONITOR'S ACRONYM(S)

USSTRATCOM - GISC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The focus of this project is to answer the question, "How should the United States government address the risks associated with dependence on foreign supplied IT hardware in critical United States networks?" Methodology included both outreach to government, security, and IT professionals, as well as independent research. The team first investigated the reasons behind the shift toward offshore hardware suppliers, finding that foreign tax benefits and incentives drive offshoring in high-tech sectors, America has been unable or unwilling to create strategy to remain on par with global trends towards incentivizing domestic manufacture, and American dominance in science and mathematical disciplines has declined. Following these findings, the team broke the hardware problem into supply chain phases, because the various stages in the IT hardware supply chain are vulnerable to subversion and counterfeiting methods to differing extents. The team's recommendation is to employ a holistic combination of a variety of technological and policy tactics in order to ensure malicious hardware is not included in critical systems.

15. SUBJECT TERMS

supply chain, technology supply chain, malicious hardware, foreign direct investment, foreign tax benefits, education, math and science education, offshoring, critical U.S. networks, foreign IT

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. John G. Hudson II
U	U	U	UU	134	19b. TELEPHONE NUMBER *(Include area code)* 402-398-8034

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

THIS PAGE LEFT INTENTIONALLY BLANK

TABLE OF CONTENTS

TABLES

FIGURES

ACRONYMS

ACI	American Competitiveness Initiative
BAA	Broad Agency Announcement
CAE/IAE	Center of Academic Excellence in Information Assurance Education
CBP	Customs and Border Protection
CCA	Clinger-Cohen Act
CIA	Central Intelligence Agency
CIO	Chief Information Officer
CMOS	Complimentary Metal-Oxide Semiconductor
DARPA	Defense Advanced Research Project Agency
DFAR	Defense Federal Acquisition Regulation
DHS	Department of Homeland Security
DoD	Department of Defense
DoE	Department of Energy
DSB	Defense Science Board
ED	Department of Education
EU	European Union
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FDI	Foreign Direct Investment
GAO	General Accountability Office
GATT	General Agreement on Tariffs and Trade
GDP	Gross Domestic Product
GSA	General Services Administration
HFDI	Horizontal Foreign Direct Investment
IA	Information Assurance
IC	Integrated Circuits
IDA	Industrial Development Agency
IP	Intellectual Property
IPR	Intellectual Property Rights
IT	Information Technology
JFCC-NW	Joint Functional Component Command Network Warfare
MID	Manufacturer's Identification
MNE	Multi-National Enterprise
NAFTA	North American Free Trade Agreement
NASA	National Aeronautics and Space Administration
NCLB	No Child Left Behind
nm	Nanometer
NSA	National Security Agency
NSF	National Science Foundation
OASD (NII)	Assistant Secretary of Defense for Networks and Information Integration

OECD	Organisation for Economic Cooperation and Development
OFPP	Office of Federal Procurement Policy
PCAST	President's Council of Advisors on Science and Technology
PPP	Purchasing Power Parity
PUF	Physical Unclonable Function
R&D	Research and Development
RFID	Radio Frequency Identification
SFS	Scholarship for Service
SMIC	Semiconductor Manufacturing International Corporation
STEM	Science, Technology, Engineering, and Mathematics
TAPO	Trusted Access Program Office
UIUC	University of Illinois at Urbana-Champaign
UPC	Universal Product Code
USTR	United States Trade Representative
VAT	Value Added Tax
VFDI	Vertical Foreign Direct Investment
VIF	Variance Inflation Factor
WAN	Wide Area Network
WHO	World Health Organization
WTO	World Trade Organization

PREFACE

This report is the product of the Global Innovation and Strategy Center's (GISC) Internship program. This program builds teams consisting of graduate and undergraduate students with the goal of providing a multidisciplinary, unclassified, non-military perspective on important Department of Defense issues.

The Summer 2008 U.S. Reliance on Foreign IT Hardware team, composed of students from Creighton University, the University of Nebraska at Omaha, and the University of Nebraska-Lincoln, was charged with evaluating the impact of U.S. reliance on foreign IT in critical U.S. networks and systems.

This project took place between late May and early August of 2008, with each team member working approximately forty hours per week. While the GISC provided the resources and technology for the project, development of the project design, conducting research and analysis and providing recommendations were all left solely to the team's discretion.

EXECUTIVE SUMMARY

For years, information technology professionals have waged an ongoing battle with software subversion, whether in the form of viruses, trojans, or various forms of malware. Hardware security, meanwhile, has very little presence in public consciousness. As our IT hardware components have increasingly been produced offshore, our vulnerability with respect to counterfeit and subverted hardware has increased by a commensurate measure. Exploitation of this vulnerability could have potentially devastating effects if a malicious piece of hardware was included in a critical system.

The focus of this project is to answer the question, "How should the United States government address the risks associated with dependence on foreign supplied IT hardware in critical United States networks?" The team was allotted eleven weeks in which to research, write, and brief the client. Methodology included both outreach to government, security, and IT professionals, as well as independent research.

The team first investigated the reasons behind the shift toward offshore hardware suppliers, finding that:

- Foreign tax benefits and incentives drive offshoring in high-tech sectors
- America has been unable or unwilling to create strategy to remain on par with global trends towards incentivizing domestic manufacture
- American dominance in science and mathematical disciplines has declined

Following these findings, the team broke the hardware problem into supply chain phases, because the various stages in the IT hardware supply chain are vulnerable to subversion and counterfeiting methods to differing extents. Design, installation, and use are significantly more within our control than manufacture, assembly, acquisition, and shipping. Each of these areas was explored so that areas of vulnerability could be identified and viable solutions to address potential threats could be devised.

The team's recommendation is to employ a holistic combination of a variety of technological and policy tactics in order to ensure malicious hardware is not included in critical systems. Among the key recommended approaches are:

- Enhancements and incentives for math and science education
- Improved government and security community outreach to "geek culture"
- Incentives for domestic design and manufacturing
- Trusted foundry programs
- Hardware "fingerprints" through Physical Unclonable Functions (PUFs)
- Side-channel verification techniques at manufacture and installation
- Cooperative authenticity verification with trusted suppliers
- Component tracking with improved radio frequency identification (RFID) technology

INTRODUCTION

Globalization, as a trend, is changing the way that government and businesses operate. In the United States, the outsourcing of products and services is becoming routine across many industrial sectors. The benefits of this practice are felt both at home and abroad; domestic companies remain competitive by sourcing components, labor, and services in less expensive countries, and those countries experience an influx of American wealth comparative to local standards.

Nowhere has this trend become more evident than in the manufacture of hardware components for information technology (IT). Information technology, like globalization, is a concept which has given much to American business. Aside from creating an entirely new economic sector, IT has provided incalculable gains in productivity for businesses across all sectors. The impact of IT reaches far beyond the bottom lines of big businesses, however, and into the life of every American. Not only does IT run the critical infrastructure that provides for electricity, water, and heat, to American citizens, it also offers operational and data support for government and military operations that provide national security.

It is the very pervasive nature of U.S. dependence on IT that leaves the nation vulnerable to various IT exploits. While software hacking garners a good deal of attention, opportunities to disrupt critical systems and services through subversion of hardware continue to proliferate. It is this risk that this report examines.

Anecdotal Evidence

Anecdotal evidence supports the notion of subverted hardware. When operating in an open source realm, locating information on specific examples of subversion is problematic. Reports on this topic are typically classified or are being evaluated as part of ongoing law enforcement investigations. Examples of counterfeiting in IT hardware are somewhat easier to find, as they are often reported after an investigation has concluded, though awareness to this problem is still limited.

One particular example of counterfeit IT hardware, and the threat that it harbors, was summarized in a recent Federal Bureau of Investigation (FBI) report concerning counterfeit Cisco products.[1] A variety of individuals and companies were involved in selling counterfeit routers, switches, gigabit interface converters, and wide area network (WAN) interface cards to military agencies, military contractors, and electric power companies in the U.S.[2]

This report suggested that a variety of individuals representing companies based in China used complexities within the procurement process to supply counterfeit items to these entities. The counterfeit products were quite sophisticated, mimicking most, if not all, of the aspects of the genuine product.[3] However, their presence was detected as a variety of compatibility and failure issues began to emerge when the products were installed in

---

[1] Roldan, Raul. "FBI Criminal Investigation: Cisco Routers." Power Point Presentation (2008).
[2] Markoff, John. "F.B.I. Says the Military Had Bogus Computer Gear." The New York Times. 9 May 2008. 17 June 2008.
[3] Markoff, John.

offices within the FBI, the Marine Corps, the Air Force, the Federal Aviation Administration, defense contractors, universities, and financial institutions. The FBI estimated that the value of the products involved in the specific cases totaled over $76 million.[4] While the motive for this effort appeared to have been purely profit driven, this example does provide evidence of the vulnerability of critical U.S. networks to counterfeit or subverted hardware.

Furthermore, an example of the possibility of producing subverted hardware was provided by an academic paper published by researchers at the University of Illinois at Urbana-Champaign (UIUC). This paper details the efforts of a team of computer scientists to build a subverted chip. Using an existing chip design as a template, the scientists introduce exceptionally small segments of circuitry into open spots on the chip. The chip included three trojans, one of which was designed to give an attacker "complete and high level" access to a computer in which the chip was installed. The researchers suggested that such trojans were "more practical, flexible, and harder to detect: than previously believed.[5]

These examples, while inferential, suggest that counterfeiting has the ability to present the U.S. with a significant threat. Classified information may reveal additional insight into the extent of counterfeiting and subversion activities.

---

[4] Rybicki, Jim. Departments of Justice and Homeland Security Announce International Initiative Against Traffickers In Counterfeit Network Hardware (Press Release). Federal Bureau of Investigation. Washington Field Division. 2008.
[5] King, Samuel T, et al. "Designing and Implementing Malicious Hardware." University of Illinois (2006).

Research Question

The research question posed to the team by the Joint Functional Component Command-Network Warfare (JFCC-NW) asks:

> "How should the United States address the risk associated with the placing of foreign manufactured IT hardware in critical U.S. networks?"

As the trend of increasingly relying on foreign manufactured IT hardware continues to expand, this question is of great importance. It is vital for the U.S. to address vulnerabilities in its networks as adversaries improve their cyber warfare capabilities. While some academic, military, and intelligence experts have begun to examine the issue of IT hardware in this context, much of the focus remains on software or internet-based attacks.

This paper addresses the research question with a multifold research methodology designed to examine a variety of factors that influence the level of risk associated with foreign manufactured IT hardware. These factors include policies, procurement strategies, supply chain issues, and political and economic environment. Special attention will be paid to technical analyses and educational enhancements that may reduce the risk associated with the current situation.

Definitions

In order to provide a baseline for discussion of the threats posed by the inclusion of

foreign hardware in U.S. critical systems, it is necessary to provide standard definitions upon which further discussion is based.

- **Hardware:** Hardware refers to the physical parts of a computer and related devices; split into internal devices (or *components*) and external devices (or *peripherals*).[6]

- **Software:** Software is a general term used to describe computer programs, including applications, scripts, and instruction sets.[7] Software can be installed by hardware vendors before purchase (a common practice with operating systems) or installed after purchase by the end-user.

- **Firmware:** Firmware is a software program specific to and existing within a hardware device.[8] For some classes of hardware, firmware is programmed into the device by the manufacturer and is never changed; for others, particularly the consumer networking peripherals, end-users may update firmware versions themselves though a manufacturer or vendor download.

- **Integrated Circuit (IC):** A hardware product, "having transistors and other circuitry elements, which are inseparably formed on a semiconductor material or an insulating material or inside the semiconductor material and designed to perform an electronic circuitry function."[9] Often simply referred to as a "chip" or "microchip," ICs may include processors, memory, and other self-contained components within computer systems.

- **Counterfeiting:** Product counterfeiting (as distinguished from currency counterfeiting), as used in this report, is defined as, "misrepresentation of the

---

[6] "Hardware Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/hardware>
[7] "Software Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/software>.
[8] "Firmware Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/firmware>.
[9] "The Semiconductor Integrated Circuits Layout Designs - IPR Toolkit." US Embassy New Delhi, India. U.S. State Department. 11 Aug. 2008 <http://newdelhi.usembassy.gov/iprsemicond.html>.

origin or nature of goods, whether through the false use of trademarks, service marks, labels of origin, artists' signatures, authentication marks, etc., or by the unlawful imitation of the appearance of packaging of goods produced by others when that appearance is protected under copyright or patent law, or by other provisions of law."[10]

- **Subversion:** The Department of Defense (DoD) defines subversion as, "action designed to undermine the military, economic, psychological, or political strength or morale of a regime. However, this definition is specific to military and political contexts."[11] In the context of computing, the definition is similar: subversion is an action designed to undermine the desired or required behaviors of the hardware, firmware, or software systems of a piece of technology.

- **Trojan:** More commonly used in software; "a program that conceals harmful code. A trojan horse usually resembles an attractive or useful program that a user would wish to execute."[12] For the purposes of this report, "trojan" will refer to a *hardware* trojan, malicious circuitry inserted into an otherwise trusted design in order to conditionally trigger a malfunction (undesirable effect).[13] The parallels between the novel hardware trojan and common software trojan are plain: both involve malicious inclusions concealed in otherwise useful and desirable products.

---

[10] "Product counterfeiting." Global Legal Information Network. Library of Congress. 31 July 2008 <http://www.glin.gov/subjecttermindex.action>.
[11] United States. Department of Defense. Department of Defense Dictionary of Military and Related Terms (JP 1-02). 30 May 2008. 14 July 2008 <http://www.dtic.mil/doctrine/jel/doddict>.
[12] Wack, John P., and Stanley A. Kurzban. NCSL Bulletin: Advising users on computer systems technology. National Institute of Standards and Technology. National Computer Systems Laboratory. 1990. National Institute of Standards and Technology. Aug. 1990. 31 July 2008 <http://csrc.nist.gov/publications/nistbul/csl90-08.txt>.
[13] Wolff, Francis, Chris Papachristou, Swarup Bhunia, and Rajat S. Chakraborty. "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme." Case Western Reserve University, Cleveland, Ohio, USA, Design, Automation and Test in Europe, 2008 (DATE '08), 10-14 Mar. 2008, Munich, Germany. 1362-365.

- **Vulnerability:** In information systems, "a weakness in information system security design procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system."[14]

- **Threat:** The DoD indirectly defines threat by defining *threat analysis* as, "in antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting…"[15] The implicit definition of threat, then, depends on the presence of an actor or agent with the capability to target US assets.

- **Attack:** "Actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities."[16]

[14] United States. Department of Defense. Department of Defense Dictionary of Military and Related Terms (JP 1-02). 30 May 2008. 14 July 2008 <http://www.dtic.mil/doctrine/jel/doddict>.
[15] United States. Department of Defense. Department of Defense Dictionary of Military and Related Terms (JP 1-02).
[16] Wilson, Clay. United States. Foreign Affairs, Defense, and Trade Division. Congressional Research Service. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 1 Apr. 2005. 24 July 2008 <http://usinfo.state.gov/infousa/government/overview/docs/RL32114.pdf>.

STATE OF AFFAIRS

The U.S. dependence on foreign IT products has many potential consequences born of several root causes. A holistic approach to understanding the problem and addressing the issue is necessary; for this reason, all major aspects of these causes and repercussions are explored. For example, focusing on technological aspects of the problem to the exclusion of policy aspects would undermine eventual solution sets. In order that the entirety of the problem is given proper attention, this report explores technological, economic, policy, and cultural background and implications for the hardware subversion and counterfeiting threat.

Technological Overview

At the time of this report, two salient characteristics of hardware components define the struggle between potential attackers and those securing the technology. First, hardware is almost overwhelmingly complex. Intel Corporation quoted nearly 600 million transistors on its latest microprocessors,[17] and the latest manufacturing processes create circuitry in the 45-nanometer (nm) range – less than 1/200th the width of a human hair.[18] A good deal of manufacturing finesse is required for the production of any product at this scale, but it is a skill that is within foreign reach. Semiconductor Manufacturing International

[17] Parker, Ron. Foreign IT Roundtable, Washington, D.C. 4 June 2008. Interview conducted by the authors.
[18] Intel Corporation. "Fun facts: Exactly how small (and powerful) is 45 nanometers?" Fact sheet. Nov. 2007. 12 Aug. 2008 <http://www.intel.com/pressroom/kits/45nm/intel45nmfunfacts_final.pdf>.

Corporation (SMIC) of China recently licensed the entirety of IBM's line of 45nm bulk complementary metal-oxide-semiconductor (CMOS) logic for production at their foundries in Shanghai and Beijing. These chips can be used in mobile devices, graphic chips, and chipsets, as well as in other consumer devices.[19]

The complexity of modern hardware is only half of the story; hardware is also generally closed. For example, ICs are encapsulated – coated with layers of resins.[20] This serves both to protect the circuit from natural damage and post-manufacture tampering, and to protect the intellectual property invested in the chip design.

The complex, closed nature of hardware works against both those who would subvert ICs and those who would defend against subversion attempts. Complexity increases the investment of time, money, and intellectual assets required to inject malicious circuitry into a device; such increases also make detection of such attempts more difficult by a commensurate measure. Similarly, closing hardware via encapsulation makes post-manufacture tampering difficult, but also means that many trojan detection methods will be correspondingly difficult and require destruction of the hardware itself.

The technological challenges presented by hardware subversion vary according to the methods used to undermine our technology. For clarity, the team is adopting a taxonomy developed by researchers at the University of Connecticut and the University of New Mexico in "Detecting Malicious Inclusions in Secure Hardware: Challenges and

---

[19] Semiconductor Manufacturing International Corporation. "SMIC and IBM Sign Licensing Agreement." Press release. 26 Dec. 2007. 12 Aug. 2008 <http://www.prnewswire.com/cgi-bin/stories.pl?acct=104&story=/www/story/12-26-2007/0004727846&edate=>.

[20] "Asymtek Applications Chip Encapsulation." Asymtek. 2008. 12 Aug. 2008

Solutions."[21] In brief, malicious hardware inclusions, or trojans, can be classified according to five characteristics:

- Type
- Size
- Distribution
- Activation
- Action[22]

A hardware trojan may be one of two types: parametric or functional. A functional trojan modifies hardware function by introducing or removing transistors or gates, such that the ultimate functionality of the circuit would be changed in some systemic way. For example, a functional trojan may redirect information to alternate storage channels, or subject information to additional mathematical functions. A parametric trojan modifies existing gate structure, specification, or arrangement such that the operating parameters of the circuit are changed. For example, wires may be thinned so that normal operating temperatures cause circuits to overheat.[23]

Next, hardware trojans vary in size (from small to large). A small trojan may consist of modification, addition, or deletion of only a few circuits, while a large trojan would consist of many such circuits. This is an important distinction for activation purposes;

---

[21] Wang, Xiaoxiao, Mohammad Tehranipoor, and Jim Plusquellic. "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions." University of Connecticut and University of New Mexico, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 9 June 2008, Anaheim, CA.
[22] Wang, Tehranipoor, and Plusquellic.
[23] Wang, Tehranipoor, and Plusquellic.

smaller trojans are more likely to be activated than large trojans. To illustrate, consider a single circuit: it can be either on or off. Basing trojan activation on this single circuit would mean that the trojan activated under 50% of the possible circuit conditions. With two circuits, a trojan could activate when one was on and the other was off, which is 25% of the possible circuit conditions. Generally, for a trojan having *a* activation conditions and *n* circuits, the possibility of the trojan being activated can be expressed as *a/(2n)*, so the likelihood of activation shrinks exponentially as trojans increase in size. [24]

Third, trojans may vary in distribution across the overall circuit. A loose distribution would indicate that trojan components were spread widely across the physical topology of the circuit, and a tight distribution would indicate that trojan components were placed topologically near each other on the circuit.[25]

Fourth, trojans may differ in activation methods. On the one hand, trojans may be externally activated, usually by an antenna or receiver apparatus. On the other hand, trojans may be activated internally, either as a function of being "always on" or based on some condition within the hardware. These conditions may be sensor-based, prompting activation when temperature, voltage, electromagnetic interference, or any other external condition is met. They may alternatively be logic-based, dependent on an internal state of

[24] Wang, Tehranipoor, and Plusquellic.
[25] Wang, Tehranipoor, and Plusquellic.

the system, a specific time on the system clock, or a particular set of input, instructions, or interrupts from the user or other connected systems.[26]

Finally, trojans differ in action characteristics, or what they are designed to do. Trojans may modify functionality, either by adding or bypassing what the circuitry is supposed to do. Alternately, they may modify specifications, introducing defects or undermining reliability. Lastly, they may be designed simply to exfiltrate information.[27]

The importance of distinguishing trojans based on these characteristics lies in what can be done with such a system of classification – namely, build a set of criteria by which trojan detection methods can be measured. Manufacturers perform functional verification on ICs as a quality control measure. That is, they test that each chip has been manufactured to perform the functions it has been designed to perform within certain environmental parameters, such as a range of temperatures. This type of functional verification that is performed is *positive*: it confirms that the chip can do what it should. *Negative* functional verification – proof that a chip performs no *extra* functions – is essentially impossible to implement exhaustively due to circuit functionality constraints. A single transistor may only perform one simple function, such as amplifying or switching a signal, based on one or more inputs and one or more outputs. The more complex functions performed by chips arise from the dense arrangements, could change the outcome of that function in a vast number of ways in response to a complex and

---

[26] Wang, Xiaoxiao, Mohammad Tehranipoor, and Jim Plusquellic. "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions." University of Connecticut and University of New Mexico, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 9 June 2008, Anaheim, CA.
[27] Wang, Tehranipoor, and Plusquellic.

singular arrangement of inputs. For example, a few transistors could be added to circuitry that performed encryption functions, leaving out critical steps that would ensure confidential messages were appropriately encrypted for security. Discovering this functionality would require one of two approaches: the first approach is to exercise all in puts of the circuitry in every possible permutation; the second approach requires knowing the types of exploitive circuitry or behaviors that should be tested ahead of time. However, because modern ICs have hundreds of millions of circuits, the number of possible permutations is so large that exercising them all would take an impractical amount of both time and resources. Additionally, testing for known exploits is approximately how most modern anti-virus software works – it checks files and behaviors on a system against a list of malicious files and behaviors. This leaves users dependent on having updated lists of exploits, and moreover, vulnerable to “zero-day” hacks – attacks which are executed before those responsible for securing the systems have any knowledge of the exploit.

An alternative to functional verification is side-channel verification, which works by examining circuit parameters. Chips containing additional or modified circuitry will behave differently than chips without these modifications. Altered chips will inevitably reveal themselves in one or more of several ways: by drawing a different amount of power, running at a different temperature, exhibiting different signal transmission times (called *circuit delay*) across areas of the chip, or emitting a different amount of electromagnetic interference (EMI). Some of these property differences may be accouted for by adversary countermeasures, but further attempts to compensate for alterations

made to one paratmeter are likely to interfere with one another. A clear advantage to side-channel verification is that it does not require exhaustive testing of every possible permutation of inputs to the circuit, nor does it require foreknowledge of possible or likely exploits.

Recommendations, beginning on page 65, will discuss the effect of such methods in ensuring the security of IT hardware.

Current Policy

Critical networks within the United States are found in both the public and private spheres, with the latter owning approximately 85% of crucial domestic infrastructure.[28] The U.S. government is limited in its role with regards to securing private networks. For instance, the National Cyber Security Division at the Department of Homeland Security (DHS) provides support and recommendations to private owners of critical networks, but cannot directly manage security operations.[29] Strides towards greater oversight of essential domestic assets are underway, as noted in the "mandatory and enforceable" cyber security reliability standards issued by the Federal Energy Regulation Commission in January 2008.[30] Focusing on the nation's bulk power operations, the new Department

[28] United States. Government Accountability Office. 2006. Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by by Sectors' Characteristics. October 2006.
[29] Personal interview with Department of Homeland Security officials. 10 July 2008.
[30] "News Release: January 17, 2008: FERC approves new reliability standards for cyber security." United States Department of Energy, Federal Energy Regulatory Commission. <http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.pdf>

of Energy (DoE) regulations include critical cyber asset identification, personnel training, and incident response planning.[31]

In the wake of President George W. Bush's cyber initiatives issued in January 2008,[32] [33] a great deal of government focus has turned towards cyber and information security.[34] These efforts highlight the need to focus on specific assets of cyber security itself: namely, network hardware. Unlike the emerging world of cyber operations, computer hardware and its associated peripherals have been in production for decades, and the legal and policy blueprints that govern them date back over 75 years.[35] Hardware manufacturing guidelines, import regulations, and trade standards began with items with specialty metals, important to the American steel and ore industries before IT was born. Once computers began to shape communications and commerce, those existing guidelines were adopted to fit the cyber realm. In the early days of computing, this policy coverage was not problematic, but today's levels of network sophistication call into question the age and intent of early legislation.

---

[31] "News Release: January 17, 2008: FERC approves new reliability standards for cyber security."
[32] Federation of American Scientists, "Intelligence Resource Program" National Security Presidential Directives, George W. Bush Administration, August 12, 2008.
[33] National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 are classified documents, but are referred to frequently in open-source literature as the current administration's executive "cyber initiative."
[34] United States. Government Accountability Office. 2006. Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by by Sectors' Characteristics. October 2006.
[35] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 21, 2005.

The uniform codification for the immense volume of legislation surrounding executive acquisition is found in the Federal Acquisition Regulation System (FAR), governed by the Office of Federal Procurement Policy (OFPP), U.S. Code Title 41.[36] Administrators with the DoD, the General Services Administration (GSA) and the National Aeronautics and Space Administration (NASA) all hold joint authority to maintain and revise the FAR.[37]

Within the DoD itself, the office of the Defense Procurement, Acquisition Policy and Strategic Sourcing (DPAP) is responsible for reviewing procurement issues surrounding weapons programs and automated information systems.[38] DPAP acts as the primary advisor to the following principles within the DoD:[39]

- Under Secretary of Defense for Acquisition, Technology, and Logistics
- Deputy Under Secretary of Defense for Acquisition and Technology
- The Defense Acquisition Board

Subordinate to DPAP is the Defense Acquisition Regulations Systems (DARS), which works to maintain existing rules to aid the acquisition workforce within the DoD.[40] Both

---

[36] United States Code: Title 41, Chapter 7. Cornell University Law School. <http://www4.law.cornell.edu/uscode/html/uscode41/usc_sup_01_41_10_7.html>
[37] "Authority of the FAR." Federal Acquisition Regulation, n.d.
[38] United States Department of Defense. Defense Procurement, Acquisition Policy, and Strategic Sourcing. <http://www.acq.osd.mil/dpap/index.html>
[39] United States Department of Defense.
[40] United States Department of Defense. "About Defense Acquisition Regulations System." Defense Procurement, Acquisition Policy, and Strategic Sourcing." <http://www.acq.osd.mil/dpap/dars/about.html>

DoD and NASA maintain agency-specific supplement to the FAR; the DoD supplement, of Defense Federal Regulation Acquisition Supplement (DFARS), carries with it the same force and effect of law as the FAR itself, as held by the Court of Federal Claims.[41]

To clarify, the DPAP structure resembles the following:

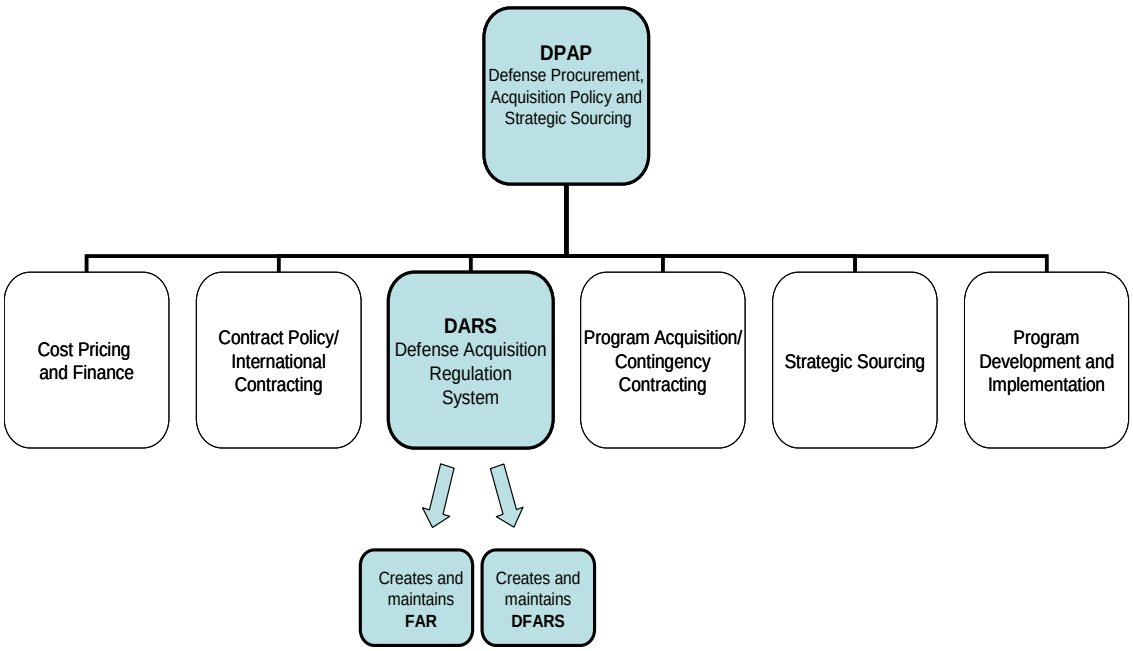

Figure 1: DPAP Structure

The following section describes the backbone of major policies that govern both the FAR and DoD regulations for procurement.

[41] *Davies Precision Machining Inc. v. U.S.*, 35 Fed. Cl. 651, 1996.

The Buy American Act

The Buy American Act (Buy American) of 1933 is "the principled domestic preference statute governing most procurement by the federal government."[42] Designed to protect the American manufacturing industry, Buy American gives preference in government procurement to domestically produced and manufactured products.[43] The Act utilizes a two-part test to identify domestic end products,[44] requiring that purchases "contain less than fifty percent foreign inputs."[45] Buy American applies only to federal contracts implemented within the U.S.[46]

Built into Buy American are multiple exceptions, several of which are considered primary.[47] Buy American does not apply to:

- Procurements where application would not be inline with public interests, or where cost is deemed unreasonable
- Products purchased for use outside the U.S.
- Procurements under $2,500
- Products which are not domestically produced in sufficient quantity or quality

---

[42] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 21, 2005.
[43] Grasso, Valerie Bailey.
[44] Federal Acquisition Regulation, Part 25, Subpart 25.1, Section 25.104. (FAC 2005-13): 25.1-5.
[45] Cooper, W.H. "Government Procurement and U.S. Trade Policy. Congressional Research Service Report for Congress. March 10, 1995.
[46] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 30, 2008.
[47] Tatelman, Todd B. "International Government-Procurement Obligations of the United States: An Overview." CRS Report for Congress, May 17, 2005.

For the latter category, hundreds of items are officially designated under Buy American as "nonavailable" for general procurement purposes, meaning that "domestic sources can only meet 50 percent or less of total U.S. Government and nongovernment demand."[48] One class of these items is microprocessor chips used in government construction.[49]

The "nonavailability" waiver is one of many existing exceptions applied to Buy American, though the history of the legislation *itself* is rife with exceptions. In the Trade Agreements Act of 1979, Congress approved the General Agreements on Tariffs and Trade (GATT) Procurement Code.[50] Not only did the GATT Procurement Code expand presidential jurisdiction over foreign trade accords,[51] it also gave the president authority to "waive procurement restrictions such as [Buy American] in implementation of international obligations."[52] Fourteen years later, however, the North American Free Trade Agreement (NAFTA) Implementation Act rendered that presidential waiver moot in the case of small business and affirmative action contracts.[53] The free trade controversies that may have mired Buy American from its passage – from lack of

[48] Federal Acquisition Regulation, Part 25.
[49] Federal Acquisition Regulation, Part 25, Subpart 25.1, Section 25.104. (FAC 2005-13): 25.1-6.
[50] Tatelman, Todd B. "International Government-Procurement Obligations of the United States: An Overview." CRS Report for Congress, May 17, 2005.
[51] "Trade Agreement Act of 1979." United States of America Department of State: International Information Programs, n.d.
[52] Tatelman, Todd B.
[53] Tatelman, Todd B.

efficacy[54] to the shield of protectionism[55] – do not appear quelled by these policy contradictions.

Buy American is often confused with the Berry Amendment of 1941,[56] an elucidation of which follows. Table 1 summarizes the main differences between the Buy American Act and the Berry Amendment.

Act	Jurisdiction	Origin Requirement	Scope
1933 Buy American Act	Most Federal Agencies	> 50 percent domestic	U.S. contracts only
1941 Berry Amendment	Defense Only	100 percent domestic	Not limited to U.S.

Table 1: Buy American Act and Berry Amendment Comparison

The Berry Amendment

While the Buy American Act is a domestic umbrella for federal acquisition overall, the Berry Amendment (Berry) governs procurement for the defense community.[57] Berry holds that:[58]

- Purchases must be 100 percent domestic in origin, and
- Contracts are not limited to the U.S.

[54] Noorzoy, M.S. "'Buy American' as an Instrument of Policy." The Canadian Journal of Economics, Vol. 1, No. 1, February 1968.
[55] Knapp, L. A. "The Buy American Act: A Review and Assessment." Columbia Law Review, Vol. 61, No. 3, March 1961.

[56] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 30, 2008.
[57] Grasso, V.B.
[58] Grasso, V.B.

Enacted on the eve of World War II, Berry was originally emplaced "to ensure that U.S. troops wore military uniforms wholly produced within the United States and to ensure that U.S. troops were fed with food products solely produced in the United States."[59] Other concerns prompting Berry surrounded the then-eight year old Buy American Act, as federal agencies were continuing to purchase foreign goods irrespective of the law.[60] Upon its approval in 1941, Berry effectively superseded prior exceptions granted to the DoD via the Buy American Act.[61]

The original legislation focusing on military uniforms was eventually expanded to include DoD procurement restrictions on food, fibers (traditional and ballistic), specialty metals, stainless steel, and other items.[62] In 2007, the specialty metal exception was shifted from Berry to a separate section in U.S. Code Title 10, specifically codifying that provision "for strategic materials critical to national security."[63] Items defined by this statue are reviewed by the Strategic Materials Protection Board, composed of officials from the office of the Secretary of Defense, the Under Secretaries of Defense for Acquisition and Intelligence, the Army, the Navy, and the Air Force.[64] The prioritization of this passage in the U.S. Code points to recognition of critical national security procurement issues at the highest levels of government decision making.

---

[59] Grasso, V.B.
[60] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 21, 2005.
[61] Grasso, V.B..
[62] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 30, 2008.
[63] Grasso, V.B.
[64] United States Code: Title 10, Subpart A, Part I, Chapter 7. Cornell University Law School.

DoD officials have long offered conflicting viewpoints of Berry, insofar as the amendment's impact on procurement efficiency and utilization.[65] Multiple proposals over the last decade reflect a desire for greater flexibility and discretion within DoD management; a common legislative "theme" was the expansion of waiver authority held by the Secretary of Defense.[66] While a 2003 General Accountability Office (GAO) report recognized Berry as benefiting the specialized needs of the defense community,[67] lawmakers had already acknowledged the need for specific legislation pertaining to IT management across the government as a whole.

A year after their initial passage in 1996 both the Federal Acquisition Reform Act (FARA) and the Information Management and Reform Act (ITMRA) were combined and renamed the "Clinger-Cohen Act,"[68] which today serves as the baseline for IT acquisition streamlining and management across the federal spectrum.[69]

The Clinger-Cohen Act

The Clinger-Cohen Act (CCA) recognizes government IT procurement as a burgeoning and vital component of federal management, emplacing statutory requirements and

---

[65] Grasso, V.B.
[66] Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 30, 2008.
[67] Grasso, V.B.
[68] Seifert, J.W. "Information Technology (IT) Management: The Clinger-Cohen Act and the Homeland Security Act of 2002." CRS Report for Congress. February 3, 2005.
[69] United States Department of Defense. "Clinger-Cohen Act and Related Documents: Foreword." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>

eliminating preexisting policy overlaps.[70] Codified in Title 40 of the U.S. Code, its main provisions include:[71]

- The removal of the General Service Administration (GSA) as the central policy and regulatory manager for federal IT purchase oversight
- The initiation of information security methods
- The first-ever[72] establishment of a department-level Chief Information Officer (CIO) for government agencies

The conceptual basis for the CIO was drawn not to implement a complete overhaul of federal IT system management overnight, but rather to "reduce risk and enhance manageability" through incremental processes.[73] Given the size and scope of federal procurement budgets, the CCA decree to move forward in a measured fashion might indicate private sector influence; one analysis called the CCA a "major step away from cost-based negotiated contracts and toward price-based competition" in the defense sector.[74] Indeed, from the DoD perspective, CIOs are "architects" for DoD-wide information policy and strategy, responsible for apportionment of IT resources into "war fighting, intelligence, business and enterprise information environment mission areas."[75]

---

[70] Seifert, J.W.
[71] United States Code. Title 40, Subtitle III, Chapter 113. Cornell University Law School.
[72] United States Department of Defense. "Clinger-Cohen Act and Related Documents." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>
[73] United States Department of Defense. "Clinger-Cohen Act and Related Documents: Foreword." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>
[74] McGowan, A.S. and Vendryzk, V.P. "The Relation Between Cost Shifting and Segment Profitability in the Defense-Contracting Industry." The Accounting Review, Vol. 77, No. 4, October 2002, pp. 949-969.
[75] Grimes, J.G. "Clinger-Cohen Act (CCA), US Title 40, Knowledge Fair III, NDU/IRMC," Assistant Secretary Defense for Networks and Information Integration, June 27, 2006.

Such efficient partitioning efforts point to the "business" model of government. A 2001 DoD review of the measure five years after its passage highlighted results-based management methodologies of the CCA.[76]

The CCA was intended to assist with IT acquisition management, and was therefore not aimed at confronting the developing risks associated with IT in critical systems. Additionally, the CCA does not apply to certain national security systems as defined in Title 40, with the exceptions of capital planning, investment control and results-based management.[77] To the "maximum extent practicable" that the CCA *does* apply to national security systems, a 2005 DoD assessment found confusion in regards to overlapping technologies, asking, "how do CCA elements apply when IT is embedded in another system?"[78] Though the CCA may be regarded as a leading law addressing IT and government acquisitions,[79] separate legislation exclusively dedicated to hardware security may be warranted.

Interestingly, at the ten-year anniversary of CCA, federal IT spending had increased an average of nine percent annually; cited factors included both cyber security and outsourcing.[80]

---

[76] Laychus, J., May, B. and Sadauskas, L. "Clinger-Cohen Act Implications for the Business Manager." United States Department of Defense, Deputy CIO PowerPoint, 2001.
[77] United States Code: Title 40, Subtitle III, Chapter 111, §11103, subsection (b). Cornell University Law School
[78] United States Department of Defense. "Improving Information Technology (IT) Investment Management and Oversight: From Clinger Cohen Act (CCA) to DoD Transformation." Executive Briefing and Project Report, Deputy CIO, Commercial Policies and Oversight, Acquisition, Technology and Logistics, March 3, 2005.
[79] United States Department of Defense. "Clinger-Cohen Act and Related Documents." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>
[80] Zimmerman, B. "Acquisition of Information Technology." Defense Acquisition University, West Region, May 23, 2007.

Trusted Hardware Programs

Efforts to confront the risk of hardware subversion through government sponsored programs have begun with programs such as the NSA's Trusted Access Program Office (TAPO), established to help alleviate associated risks. The program was created to assist the DoD and others in the intelligence community with gaining access to trusted microelectronic technology components that are used in critical systems. TAPO defines trust as "the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture, and distribute national security critical components."[81]

- TAPO streamlines its efforts by focusing on five main objectives:
- Guaranteed access to trusted suppliers
- Ability to fabricate classified designs up to the secret level
- Low volume customer access to leading edge technology
- Quick turnaround times for prototyping and production
- Technology support through industry leadership.[82]

One of TAPO's most important responsibilities is locating and sustaining trusted suppliers for microelectronic parts.[83] The Trusted Foundry Program is a collaborative

---

[81] Zimmerman, B. "Acquisition of Information Technology." Defense Acquisition University, West Region, May 23, 2007.
[82] National Security Agency. "Trusted Access Program Office (TAPO)." May 2008. <http://www.nsa.gov>
[83] "TAPO Welcome Page." TAPO: Trusted Access Program Office. 2 July 2008 <https://www.tapoffice.org/tapo.html>.

effort of the NSA and DoD and was established to tackle the increasing problem of offshore semiconductor manufacturing. The program is also responsible for regulating and maintaining domestically owned and operated manufacturing plants. The Trusted Foundry Program has established a working relationship with IBM in order to produce advanced microelectronic components in a trusted environment, and insures these capabilities until fiscal year 2013, though what the government will do after 2013 is still unclear.[84] [85]

In addition to the preceding programs, the Defense Advanced Research Project Agency (DARPA) has created a program to examine the essential problem facing the United States' reliance on foreign manufactured semiconductors – ensuring trusted integrated circuits in critical U.S. networks. DAPRA's TRUST in Integrated Circuits program seeks to determine whether a microchip that was manufactured in an untrusted environment or process that is outside of US control can be trusted to perform operations only as specified by the design and no additional malicious circuitry. Though DARPA recognizes the importance of the Trusted Foundry Program, it continues its quest to define a technological approach to verify a microchip in the absence of a trusted foundry.[86]

---

[84] National Security Agency.
[85] "TAPO Welcome Page."
[86] Microsystems Technology Office. "Trust in Integrated Circuits (TIC)." 7 March 2007. <http://www.darpa.mil>

Import Regulations

IT hardware is subject to the same import regulations as other products imported into the United States. Although potential technological solutions exist on both ends of the supply chain to either prevent malicious inclusions from being added to the hardware at inception or to keep subverted or counterfeited hardware from being added to a critical network, few techniques are tenable for the stages in between. Pharmaceutical drugs that are manufactured offshore encounter the same problems as IT hardware; manufacturers possess techniques that greatly reduce the chances that a drug has been tampered with at production as well as individual testing by pharmacies and distributors before the product is given to customers. However, in an effort to reduce the amount of bad product from actually entering the U.S. supply, the federal government through the Food and Drug Administration (FDA) has built in policies that increase the oversight on imported drugs as well as the FDA's ability to test and deny importation to questionable shipments of drugs. And although the import regulations are not perfect in preventing all bad products from entering the U.S. supply, they provide a framework upon which import regulations specific for IT hardware imports could be tailored. For this reason, the nature and implications of U.S. import regulations are explored to provide comparable solutions for IT hardware.

The World Health Organization (WHO) defines a counterfeit medicine as "a medicine that is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients,

without active ingredients, with insufficient active ingredients or with fake packaging."[87]

To achieve maximum patient safety, the FDA, Customs and Border Protection (CBP), Homeland Security, and individual states regulate the industry through laws and administrative orders designed to protect the integrity of drugs through all stages of the pharmaceutical supply chain.[88] These laws and regulations require documents to accurately record the flow of drugs from manufacture to consumption. Inherent in the process are the requirements for "track" and "trace".[89] "Tracking" involves knowing the physical location of a particular drug within the supply chain at all times; "tracing" is the ability to know the historical locations, the time spent at each location, record of ownership, packaging configurations, and environmental storage conditions for a particular drug.[90] These functions of the supply chain form the groundwork for improved patient safety by giving manufacturers, distributors, and pharmacies a universal method to detect and control counterfeiting, drug diversions, and other forms of mishandling.[91]

The vast majority of drugs sold in the U.S. are safe, although the industry is quite attractive to counterfeiters. However, counterfeit medications have shown up in the U.S. drug supply, including well-known drugs such as Procrit and Lipitor. Since the primary motive for producing counterfeit drugs concerns the possibility of making great profits, the ability to understand this motive has helped the FDA and states move forward in the

---

[87] "Counterfeit and Substandard Medicines." Impact: International Medical Products Anti-Counterfeiting Taskforce. 2008. World Health Organization. 18 June 2008 <https://www.who.int/medicines/services/counterfeit/en/>.
[88] "Regulatory Procedures Manual March 2008 Chapter 9 Import Procedures." ORA Import Program. Mar. 2008. US Food and Drug Administration. 24 June 2008 <http://www.fda.gov/ora/import/ora_import_program.html>.
[89] Koh, R., Edmund W. Schuster, Indy Chackrabarti, Attilio Bellman. 2003. White Paper: "Securing the Pharmaceutical Supply Chain." Massachusetts Institute of Technology, Auto-ID Center, June 1, 2003.
[90] Koh, Schuster, Chakrabarti, & Bellman.
[91] Koh, Schuster, Chakrabarti, & Bellman.

fight against counterfeit drugs. New legislation is being enacted to combat the problem; for example, Florida recently gained national attention by introducing a bill to establish a "pedigree" for each drug sold in the U.S. with the intention of verifying authenticity of the drug.[92]

Besides legislation, the pharmaceutical industry attempts to combat counterfeits using a number of different technological techniques. Most detection procedures rely on manual product inspection by pharmacists or sales representatives to check for evidence of counterfeiting; this can be expensive and time-consuming. Some drug companies have injected a chemical signature directly into medications, which can later be checked with a small handheld device similar to a home pregnancy test. Tamper-proof packaging has been used on most drug containers, which have contained holograms, difficult-to-replicate packaging designs, and unique fonts on the bottles and design.[93] Table 2 below provides several anti-counterfeiting measures that are currently used, as well as identifying their covert or overt nature, and the ease of replication.[94]

[92] Koh, Schuster, Chakrabarti, & Bellman.
[93] Koh, R., Edmund W. Schuster, Indy Chackrabarti, Attilio Bellman. 2003. White Paper: "Securing the Pharmaceutical Supply Chain." Massachusetts Institute of Technology, Auto-ID Center, June 1, 2003.
[94] Koh, Schuster, Chakrabarti, & Bellman

ANTI-COUNTERFEIT MEASURE	COVERT	OVERT	REPLICATION
Intra-Formulation			
Immunoassay	✓		Low
Unique Flavoring		✓	Low
Package Level			
Design		✓	High
Watermarks	✓	✓	High
Digital Watermarks	✓	✓	New
Fibers and Threads	✓	✓	Medium
Reactive Inks	✓	✓	Medium
Holograms, OVD	✓	✓	High
Bar Code		✓	High

Table 2: Anti-Counterfeit Measures[95]

Furthermore, the FDA is responsible for determining whether or not an article offered for importation is in compliance with or in violation of the acts enforced by the FDA. The CBP and FDA often work closely together; the CBP alerts the FDA of all formal and informal entries of FDA articles under FDA jurisdiction at ports of entry located in the district's territory.[96] Using the electronic screening process when attempting to import articles into the United States, importers are required to provide the FDA product code, the manufacturer's identification (MID) of the foreign manufacturer, the MID of the foreign shipper, and the country of origin. Any incoming shipments may be sampled for further evaluation of the product if they are deemed to fall under the Federal Food, Drug, and Cosmetic Act. If the sampling of an article offered for import has been deemed to be in violation of the act, it could be subject to refusal of admission or additional legal

[95] Koh, Schuster, Chakrabarti, & Bellman
[96] "Regulatory Procedures Manual March 2008 Chapter 9 Import Procedures." ORA Import Program. Mar. 2008. US Food and Drug Administration. 24 June 2008 <http://www.fda.gov/ora/import/ora_import_program.html>.

actions. Chapter 9-1 of the FDA Import Procedures outlines the process of declaring items for importation and the actions FDA officers may take in ensuring the validity of the product.[97]

Besides attempting to secure the whole supply chain, legislative acts such as Florida's "pedigree" program and many of the anti-counterfeit methods shown in Table 2, as well as the FDA import regulations, are designed to detect counterfeit drugs at the step that is analogous to the "instillation and use" phase in the supply chain.[98] Although a drug shipment may have been compromised at any of the other steps in the supply chain, import and testing regulations offer another chance of isolating and preventing counterfeit drugs from entering U.S. supply.

A problem arises, however, for items that do not fall under the Federal Food, Drug, and Cosmetic Act. The possibility of detecting counterfeited or subverted inventory is greatly reduced as less oversight is required for items that are not subject to the Food, Drug, and Cosmetic Act.

Economic Realities

Underlying virtually all aspects of U.S. global power, from its military dominance to its cultural appeal, is its economic strength. As Figure 2 illustrates, the U.S. accounted for a full 48%, or $711 billion, of worldwide military expenditures as of the date of the report

---

[97] "Regulatory Procedures Manual March 2008 Chapter 9 Import Procedures."
[98] "Beyond Pedigree: The Role of Infrastructure in the Pharmaceutical Supply Chain." Verisign. 7 July 2005. 6 Aug. 2008 <http://www.verisign.com/static/031078.pdf>.

in 2008.[99] U.S. soft power, or its ability to attract others by the legitimacy of U.S. policies and the values that undermine them,[100] is also directly related to American business, as multinational firms such as Disney and Coca-Cola have become international symbols of American culture. In the modern economy, U.S. power hinges on American firms' ability to actively compete on a global scale. Comparative advantages, wherever they exist, are being exploited as "multinationals are evolving into complex global enterprises, spreading their activities across value chains over different locations to take advantage of specific locational conditions."[101]

---

[99] "World Military Spending." Global Issues. 19 July 2008. <http://www.globalissues.org/Geopolitics/ArmsTrade/Spending.asp#WorldMilitarySpending>

[100] Nye, Joseph S. "The Decline of America's Soft Power." Foreign Affairs. May-June 2004. The Council of Foreign Relations. 25 Aug. 2008 <http://www.foreignaffairs.org/20040501facomment83303/joseph-s-nye-jr/the-decline-of-america-s-soft-power.html>.

[101] Council on Competitiveness. Competitiveness Index: Where America Stands. 2007. 17 July 2008. <http://www.compete.org/images/uploads/File/PDF%20Files/Competitiveness_Index_Where_America_Stands_March_2007.pdf>.

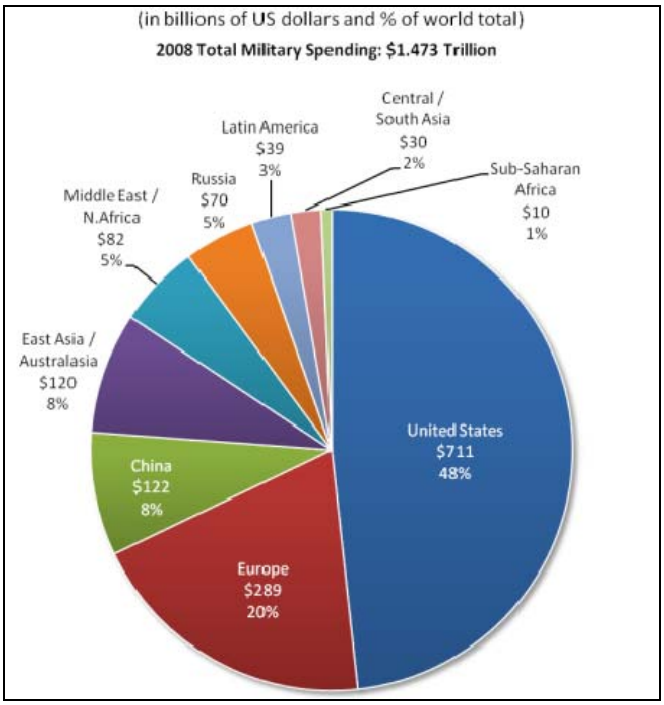

Figure 2: 2008 Total Military Spending Worldwide[102]

Manufacturing in particular has experienced a precipitous decline in the U.S. over the past 30 years as firms seek to lower costs by relocating production processes to foreign countries.[103] As Figure 3 demonstrates below, manufacturing and sales in the IT industry is increasingly located in geographic areas outside the U.S., particularly in Asia Pacific countries. However, outsourcing is no longer limited to low-skill, low-technology industries and processes. Highly specialized functions such as research and development (R&D) are performed overseas. These developments within the IT industry have implications beyond economics, for as the Defense Science Board (DSB) noted in 2005,

---

[102] "World Military Spending." Global Issues. 19 July 2008. <http://www.globalissues.org/Geopolitics/ArmsTrade/Spending.asp#WorldMilitarySpending>

[103] Nye, Joseph S. "The Decline of America's Soft Power." Foreign Affairs. May-June 2004. The Council of Foreign Relations. 25 Aug. 2008 <http://www.foreignaffairs.org/20040501facomment83303/joseph-s-nye-jr/the-decline-of-america-s-soft-power.html>.

"[t]rusted and assured supplies of integrated circuit components for military applications are critical matters for U.S. national security…"

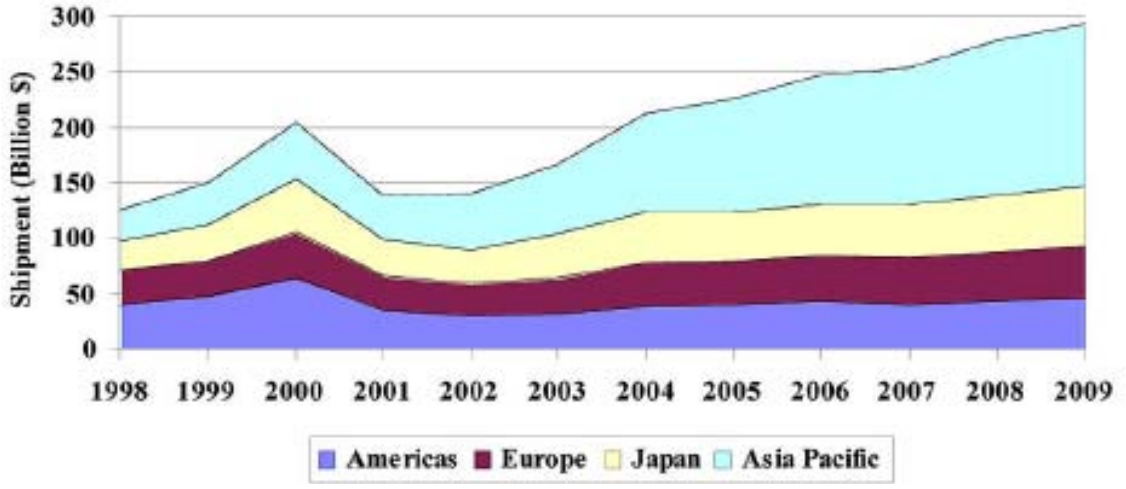

Figure 3: Changes in distribution of global semiconductor sales[104]

The following section provides an overview of the current global economic environment, with attention paid to the IT industry, and analyzes a variety of variables that influence a firm's decision to invest overseas. These include those factors that encourage and also those that dissuade FDI.

FDI Conditions

Foreign direct investment is the process by which firms invest in regions outside its home country. There are two types of FDI: horizontal and vertical. Horizontal FDI (HFDI) refers to investment in a country in order to expand into new markets; the objective is to

[104] Pope, Sydney. "Trusted Integrated Circuit Strategy." IEEE Transactions on Components and Packaging Technologies 31:1 (2008) 230-234.

increase the customer base, limit trade costs, and gain a strategic advantage over competitors. Vertical FDI (VFDI) refers to the process of moving certain functions within the production process to different geographic locations; the primary benefit of VFDI is that factor costs are reduced.[105] Although many variables affect a firm's decision to relocate production, lower labor costs are typically cited as the greatest determinant. The term "China Price" has been coined to describe the large savings multinational enterprises (MNEs) accrue due to lower labor costs in East Asian states, particularly China. Production costs in China are 30-50% lower as compared to the United States. Between 2000 and 2004, the U.S. manufacturing sector lost approximately 2.7 million jobs due to outsourcing, with many more since then.[106]

The "China Price" applies to many industries that have experienced heavy off-shoring and are labor-intensive, such as textiles. However, because the IT industry is much more capital-intensive as opposed to labor-intensive, the "China Price" does not apply in this case. For instance, the cost differential between the construction and maintenance of a semiconductor fabrication plant in China versus the U.S. is more than $1 billion over a 10-year period. Approximately 70% of the cost difference is due to tax benefits. Only 10% of the cost differential is due to lower wages.[107] Thus, for the IT industry, a state's competitive advantage comes from its tax policies – not from lower labor costs as the "China Price" predicts.

---

[105] Navaretti, Giorgio Barb and Anthony J. Venables. Multinational Firms in the World Economy. Princeton, NJ: Princeton University Press, 2004.
[106] "The China Price." BusinessWeek. Dec 2004. 19 July 2008.
[107] Scalise, George. "China's High-Technology Development." Testimony before the US China Economic and Security Review Commission. April 21, 2005.

Increased VFDI within the IT industry has largely been made possible by a shift in major actors. In the early years of the industry, the U.S. military was responsible for much of the IT R&D and use. This is no longer the case, as private firms supplying commercial markets are now the leading innovators and suppliers.[108]

Although the differences between horizontal and vertical FDI are important and substantial, the implications of VFDI in terms of hardware subversion and counterfeiting are greater than those associated with HFDI. As will be discussed in greater detail starting on page 38, greater opportunities are present for a potential subverter or counterfeiter when the manufacturing phase (as opposed to products for sale) is accessible. As such, all further discussion of FDI will be of VFDI.

Supply Chain

The supply chain provides numerous opportunities for subversion and counterfeiting of hardware. Because the United States relies more heavily on single sources and domestic suppliers for design, installation, and use of IT solutions, these portions of the supply chain are considered more secure when compared to the other phases. They are considered to be more secure because they are rarely performed offshore which increases US control, therefore implying that they are less vulnerable to foreign subversion. In contrast, manufacturing, assembly, acquisition, and shipping are increasingly offshored, providing malicious actors a multitude of opportunities to tamper with hardware.

---

[108] Pope, Sydney. "Trusted Integrated Circuit Strategy." IEEE Transactions on Components and Packaging Technologies 31:1 (2008) 230-234.

Design

The design phase of the IT hardware supply chain is typically performed domestically, even for companies that offshore other production phases. For example, in 2007, Intel Corporation announced its intent to open a chip manufacturing plant in China by 2010, but the plant will not be involved with "core technologies" or the design. It will produce only supporting chipsets instead of Intel's cutting-edge microprocessors.[109] Weak intellectual property (IP) protection laws should discourage firms from outsourcing design as well, because once the design is published, it can be replicated and therefore counterfeited or subverted.

However, as the analysis in Appendix A suggests, weak IP protection laws do not necessarily dissuade MNEs from exporting production functions. Furthermore, technical acumen is improving in many countries that have traditionally been centers of manufacturing. If the current trend continues, then the design phase may also eventually be performed offshore. Opportunities to tamper with hardware components are present in the design phase, as a malicious designer can insert additional functionality into a chip. Access to the design of a microprocessor grants an adversary the ability to potentially affect every chip produced.[110]

---

[109] Barboza, David. "Intel to Build Advanced Chip-Making Plant in China." The New York Times. 27 Mar. 2007.1 Aug. 2008 <http://www.nytimes.com/2007/03/27/technology/27chip.html>.
[110] Defense Science Board. High Performance Microchip Supply. Feb 2005. 19 July 2008. <http://www.cra.org/govaffairs/images/DSB.Appendix.D.pdf>

Manufacture and Assembly

In contrast to the design phase, IT firms have moved much of the manufacturing and assembly phases of the supply chain to locations overseas. As this process continues to expand, control and security assurance over these phases declines. An additional complication is the growing trend where less complex components are assembled and sent on for further modifications. Many cutting-edge components are manufactured in countries with the appropriate knowledge and infrastructure. Each step of component compilation may be contracted to different actors, thereby reducing the accountability for any particular supplier.

In the 1980s, companies began to outsource the production of semiconductors to overseas fabrication plants, or foundries. Taiwanese foundries emerged as a large provider of ICs, but these production capabilities are increasingly shifting to mainland China.[111] The scale of offshoring within this phase introduces several vulnerabilities; after a chip design has been sent to a foundry, a mask is fabricated. The mask, which functions as a template for IC design, is then printed onto a silicon wafer using a process called photolithography. Engineers at this stage, who often are not employees of the designing firm, gain access to the design and the ability to alter the mask: this presents the opportunity for malicious actors to subvert the IC or steal the design for counterfeiting purposes.[112]

---

[111] United States. Government Accountability Office. Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India. Sept 2006. 14 Aug 2008. <http://www.gao.gov/new.idems/d06423.pdf>
[112] Goldstein, Donald J. et al. USG Integrated Circuit Supply Chain Threat Opportunity Study. Institute for Defense Analyses. Jan 2006.

Attempts to prevent harmful activity during manufacturing and assembly run into many obstacles because the U.S. has largely exported much control of these phases to other countries. Existing quality control measures at foundries are useful but ultimately inadequate to ensure security.

Acquisition and Shipping

When products are manufactured offshore, the acquisition and shipping of these goods is also performed (in part) overseas as well. Many of the problems that arise in the manufacturing phase, namely that it is no longer in U.S. control, also apply to packaging and shipping.

Currently, Universal Product Code (UPC) barcodes are the most commonly used technique to track products. However, developments in tracking technologies have provided one possible technological solution that can log routes, handlers, and damage incurred while an item is in transit, namely, radio frequency identification (RFID). This technology has been the focus of much research as a means of providing security through the supply chain. Yet RFID chips are not fool proof, as will be discussed on page 86.[113]

Securing the acquisition and shipping phases will require continued improvement of tracking technologies and policies that ensure malicious IT components do not enter critical networks.

---

[113] Lee, Hau L. Supply Chain Security - Are You Ready? Stanford Global Supply Chain Management Forum. Sept 2004. 14 Aug 2008. <http://www.stanford.edu/group/scforum/Welcome/White%20Papers/SC_Security.pdf>.

Installation and Use

The installation and use portions of the supply chain are also less susceptible to the vulnerabilities presented by offshoring. Aside from the possibility of a domestically-sourced attacker gaining access to a critical network, these phases are effectively safe from foreign subversion or counterfeiting.

There are, however, opportunities to perform final verification procedures to ensure IT hardware has not been subverted. As hardware components are placed in essential networks, various techniques can be employed to check legitimacy and proper functionality, with further discussion to be found on page 81.

Importance of Research and Development

Economists have produced a variety of models that illustrate how an economy can sustain long term growth. In the 1950s, Nobel Prize laureate Robert Solow developed a model that emphasized the importance of technological progress. Solow found that in order for an economy to increase overall output from existing resources, the society must apply innovations. This model, however, does not specify how an economy achieves technological progress. A second growth model developed by Paul Romer illustrates how innovation is achieved. A key finding from Romer's analysis highlights the high costs of innovation and the requirement of committed resources for sustained growth.[114] Research

[114] For a detailed explanation of the growth models developed by Robert Solow and Paul Romer, see: Van den Berg, Hendrick. Economic Growth and Development. Boston, MA: McGraw Hill, 2001.

and development requires the training of scientists and engineers, laboratories, grants, equipment, and more. The IT industry provides a clear example of the implications and importance of technological innovation.

The IT industry's rapid technological advances and widespread integration into the larger economy exemplifies the growth patterns predicted by Solow's model. Productivity in particular greatly increased in the 1990s, as businesses incorporated IT technologies; researchers have found that industries that became heavily infused with IT grew 75% faster than those that did not. With respect to the American economy as a whole, the integration of IT accounts for 25-33% of the increase in real GDP growth for the entire decade.[115]

Just as American businesses benefited from the design and incorporation of IT in the 1990s, foreign businesses are currently engaged in the same process, though with substantial consequences for the U.S. economy. In January 2004, the President's Council of Advisors on Science and Technology (PCAST) released a report recommending ways to maintain and strengthen the United States' "innovation ecosystems".[116] This ecosystem is composed of R&D and manufacturing, processes that are best maximized when geographically co-located. "Clusters of innovation" emerge when an industry agglomerates; skilled workers, successful business practices, and proper infrastructure all contribute to a location's innovative spirit. The PCAST report notes that "several major

---

[115] Mann, Catherine L. and Jacob Funk Kirkegaard. Accelerating the Globalization of America The Role for Information Technology. Washington, D.C.: Institute for International Economics, 2006.
[116] The President's Council of Advisors on Science and Technology. Sustaining the Nation's Innovation Ecosystems. Jan 2004. 17 July 2008. <http://www.ostp.gov/pdf/finalpcastsecapabilitiespackage.pdf>.

manufacturers…decided to locate new plants in the United States, despite cost benefits of offshore manufacturing, due to the proximity of leading university R&D capabilities (or a state's commitment to upgrade such capabilities)." Nevertheless, evidence presented earlier illustrates the extent of outsourcing of IT manufacturing. As predicted by PCAST, R&D is relocating to sites where manufacturing has already been established, therefore weakening domestic "innovative ecosystems".[117]

Currently, U.S. firms conduct a great amount of IT R&D as measured by the share of global patents. As Figure 4 illustrates, U.S. firms accounted for approximately 50% of patents granted up to 2004.[118]

[117] AeA, Advancing the Business of Technology. Losing the Competitive Advantage? 2005. 17 July 2008. <http://www.aeanet.org/publications/idjj_CompetitivenessMain0205.asp>.
[118] Mann, Catherine L. and Jacob Funk Kirkegaard. Accelerating the Globalization of America The Role for Information Technology. Washington, D.C.: Institute for International Economics, 2006.

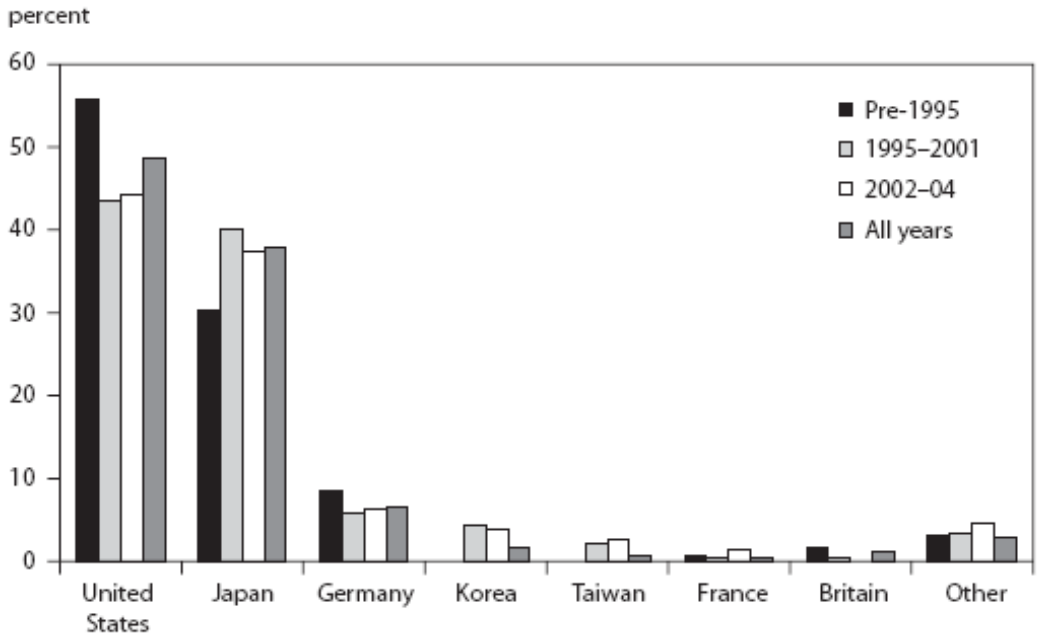

Figure 4: Share of patents granted to top 100 companies[119]

However, the continuation of this dominant position held by U.S. firms is in doubt, as the Council on Competitiveness noted in its 2007 Competitive Index:

> "With about 5 percent of the world's population and about 30 percent of world GDP, the United States is responsible for 37 percent of global R&D spending, has 29 percent of all researchers, publishes 30 percent of all scientific articles, produces 22 percent of all new doctorates in science and engineering, and attracts 31 percent of all international students. Across all of these metrics, America's share has fallen as other countries have increased their science and technology-related activities, but the United States still has a significant absolute lead in almost every category."[120]

---

[119] Mann, Catherine L. and Jacob Funk Kirkegaard. Accelerating the Globalization of America The Role for Information Technology. Washington, D.C.: Institute for International Economics, 2006.
[120] Council on Competitiveness. Competitiveness Index: Where America Stands. 2007. 17 July 2008. <http://www.compete.org/images/uploads/File/PDF%20Files/Competitiveness_Index_Where_America_Stands_March_2007.pdf>.

As the passage above suggests, the supply of American scientists and engineers is currently sufficient to maintain the United States' innovative and competitive edge. What is unclear is if the current supply of scientists and engineers is capable of maintaining America's edge in scientific innovation. Of great concern to the defense and intelligence communities is the decreasing supply of U.S.-born engineers who are eligible to receive proper security clearances for military or intelligence R&D.[121] According to the Romer model, investment in an economy's human capital stock is vital if firms and the economy as a whole are to sustain growth.[122]

As economic growth models and studies of American business competitiveness conclude, the continued strength of the U.S. economy relies heavily on a deep, renewable pool of scientists and engineers. The necessary training for these workers, however, has declined in recent years, particularly in relation to other countries.[123] The following sections provide an overview of the current state of affairs of the American education system as well as recent initiatives designed to fortify math and science education and innovative ecosystems.

---

[121] Defense Science Board. Future Strategic Strike Skills. March 2006. 17 July 2008. <http://www.acq.osd.mil/dsb/reports/2006-03-Skills_Report.pdf>.
[122] Van den Berg, Hendrick. Economic Growth and Development. Boston, MA: McGraw Hill, 2001.
[123] United States. National Mathematics Advisory Panel. Department of Education. The Final Report of the National Mathematics Advisory Panel. 2008.

Cultural Issues

Although technology is vital in solving this question regarding subverted or counterfeited hardware, several cultural factors are integral in maintaining and reversing the current trends previously discussed. Education and outreach to certain sub-cultures in American will provide the long term foundation to American security and technological intellectual capital.

Education

The prominence and security of a state are linked with its ability to create and improve upon ideas. Prominent societies have dominated the mathematical and scientific skills that led to improvements in medicine, commerce, defense, finance, and technology. During the 20th century, the U.S. dominated in terms of mathematical and scientific skills, innovations, as well as the caliber of specialists available to solve current problems.

Then, in 1957, the Russians launched Sputnik into space, beating the U.S. to the new frontier. With the possibility of the U.S. losing its technological and scientific edge over the rest of the world on everyone's minds, a greater emphasis was placed not only on ensuring that the U.S. would be the first to put a man in space, but also in guaranteeing that enough educational resources were available to entice the next generation with the possibilities that emerged from science, technology, engineering, and math (STEM) careers. However, this trend lost its fervor in subsequent years, and the lack of continued

emphasis placed on math and science education has the potential to create a possible crisis that could affect the U.S. and its position as a world leader in technology innovation.

Without enacting necessary changes to the educational system to combat declining interest in STEM careers, the U.S. could relinquish role as a leader in the 21st century. This looming crisis is evidenced by many markers: the number of American students enrolling in STEM programs in universities has experienced continual declines for many years; federal research support for engineering and physical sciences has declined by half a percentage of the gross domestic product since 1970; and other countries, especially in Asia, are aggressively increasing research funding and grants, student enrollment rates and opportunities, and the quality of programs at universities to build up a large STEM capability to direct technological advancement.[124] Such trends could place substantial stress on the America's ability to sustain a workforce of adequate size and quality. For decades, the U.S. has relied upon a great number of foreign mathematicians and scientists; however, blossoming economies and attractive job opportunities abroad make it less likely that such trends will continue.[125]

---

[124] Jischke, Martin C. "Science Education in United States Reaches a Crossroads." Purdue University News. 24 Jan. 2006. Purdue University. 8 July 2008 <http://www.purdue.edu/UNS/html3month/2006/060124.SP-JIschke.rotary.html>.

[125] United States. National Mathematics Advisory Panel. Department of Education. The Final Report of the National Mathematics Advisory Panel. 2008.

Elementary and Secondary Education

Although much attention regarding the U.S. decline in math and sciences seems to focus on higher education, math and science education begins much earlier. Education in the U.S. is not directed by the federal government in general, and curriculum is determined by individual states. The U.S. Department of Education's (ED) primary focus then is to devise and monitor federal funding of education programs and to enforce educational laws regarding privacy and civil rights. One policy that supersedes state level regulations was signed into effect January 8, 2002; the No Child Left Behind Act (NCLB) is a piece of federal legislation that reauthorized several federal programs with the principal intention of improving the performance of U.S. primary and secondary public schools by increasing the standards of accountability for states, school districts, and schools.[126] Though its intent is to improve quality and equity of education systems across the states, several issues arise that interfere with its effectiveness.

The NCLB Act requires that every state conducts annual math and reading tests to students from third to eighth grade. Instead of one standardized, national assessment test being distributed by the ED, states are able to create their own academic standards and therefore are responsible for contacting one of the five main private companies who create and score standardized tests to customize a test that suits their needs.[127] Some states are reluctant to spend money for premium, challenging tests, a fact which not only

---

[126] "No Child Left Behind." Ed.Gov. US Department of Education. 2 July 2008 <http://www.ed.gov/nclb/landing.jhtml?src=pb>.
[127] "No Child Left Behind."

causes inconsistency between the states, but also skews the results of the test. If the tests are easy, the students "pass," and the schools continue to receive federal funding. Some states use only multiple-choice questions, some include multiple-choice and short answer, some include long, open-response questions, and many use a combination of several types of test questions.[128] The threat of lost funding changes the goals from teaching well to teaching the test well. Under this act, the requirement for increased accountability means that schools must show "yearly adequate progress," and if they do not, they could incur sanctions that range from warnings to teacher dismissals to complete takeovers.[129] The possibility that testing companies may score the test incorrectly also encourages states to dumb down their tests and remove short- or- long answer tests, using only multiple-choice. Price is also a factor here, where grading an essay can range from $0.50 - $5.00 to grade, whereas a computerized multiple-choice will cost only pennies to run through a scanner.[130] The economical incentive then would be to provide only multiple-choice exams to save on grading costs. This has the potential to negatively manifest itself in children's performance on tests and through their education.

The National Mathematics Advisory Panel produced a report for the Department of Education to assess mathematic skills of U.S. students. This panel found that math literacy is a serious problem in the U.S.; this is evident not only in standardized test

---

[128] Vu, Pauline. "Do State Tests Make the Grade?" Stateline.Org. 17 Jan. 2008. 27 June 2008 <http://www.stateline.org/live/details/story?contentId=272382>.
[129] "Too Much Testing?" CBS News. 4 Apr. 2006. 18 July 2008
[130] Winerip, Michael. "Standardized Tests Face a Crisis Over Standards." Education Sector. 22 Mar. 2006. 18 July 2008 <http://www.educationsector.org/media/media_show.htm?doc_id=362581>.

scores, but also in basic math problems that most adults cannot solve.[131] For example, 78% of adults polled cannot explain how to compute the interest paid on a loan, 71% cannot calculate miles per gallon on a trip, and 58% cannot calculate a 10% tip.[132] Furthermore, it is clear from a wide variety of research that many student and even adults have problems correctly doing fractions, a skill that is foundational to success in algebra. Algebra is often considered to be the foundation on which additional math is based, and the lack of mastery for that subject prevents subsequent mastery. According to the National Assessment of Educational Progress, 27% of eighth-graders could not solve a word problem that required dividing fractions.[133]

A recurring problem that algebra teachers bring up time and again focuses on basic math skills and the fact that many students do not have the concepts mastered before entering eighth grade. This hindrance prevents children from excelling in higher-level math courses, such as calculus, while still in high school.[134] Trends such as these affect U.S. students not only at home, but also among the world theater.

The Organisation for Economic Co-Operation and Development (OECD) publishes a triennial survey of the knowledge and skills of 15-year-olds in collaborating countries that draws international comparison between the participating countries and cultures.[135] More than 400,000 students from 57 countries took part in the 2006 survey, which

---

[131] United States. National Mathematics Advisory Panel. Department of Education. The Final Report of the National Mathematics Advisory Panel. 2008.
[132] United States.
[133] United States.
[134] United States.
[135] The Programme for International Student Assessment (PISA). Organisation for Economic Co-operation and Development. 2006

focused on science. Overall, Finland was the highest performing country, followed by Canada, Japan, New Zealand, Hong Kong-China, Chinese Taipei, and Estonia. The U.S. ranked 29th overall on science skills out of the 57 countries examined with scores that were statistically significantly below the OECD average.[136] Besides just measuring actual science skills, the survey also observed student's self-concept in terms of science. Not surprisingly, students who enjoyed learning science were more likely to perform better on tests.[137] Recommendations in the area of education (see page 72) will capitalize and expand upon this fact.

Higher Education

Following the conclusion of World War II and into the Cold War, the U.S. was the undisputed leader of science and technology innovation. The American higher education system produced by far the largest amount of graduates in STEM fields. In part, these disciplines were attractive to students wishing to contribute to space race initiatives. By 1970, U.S. colleges and universities enrolled approximately 30% of post-secondary education students worldwide, and over 50% of STEM degrees were granted by U.S. institutions.[138]

Since then, however, the rest of the world has begun to close the gap, particularly in the STEM disciplines. In 2001, U.S. institutions enrolled only 14% of post-secondary

---

[136] The Programme for International Student Assessment (PISA). Organisation for Economic Co-operation and Development. 2006
[137] The Programme for International Student Assessment (PISA).
[138] Freeman, Richard B. "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?" NBER Working Paper No. 11457. June 2005.

education students. Furthermore, a larger percentage of students in most countries are enrolled in engineering fields compared to the U.S.[139] While developed economies in Europe achieved these gains decades ago, lesser developed countries are currently increasing their number of engineering students. Table 3 shows the ratio of the number of science and engineering PhD students from foreign institutions to that of U.S. institutions. As of 2001, Asian countries were quickly achieving parity.[140] Accounting for all levels of post-secondary education, China graduated over 600,000 engineering students in 2005, compared with approximately 70,000 at U.S. institutions, though the McKinsey Global Institute notes that the quality of programs at U.S. universities is higher than those at most foreign universities.[141]

---

[139] Freeman, Richard B. "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?" NBER Working Paper No. 11457. June 2005.
[140] Freeman, Richard B.
[141] McKinsey & Company. Addressing China's Looming Talent Shortage. Oct 2005. 19 July 2008. <http://www.mckinsey.com/mgi/reports/pdfs/China_talent/ChinaPerspective.pdf>.

(Ratio of PhDs in each year)	1975	1989	2001	2003[a]	2010[a]
Asia major nations	0.22	0.48	0.96		
China	na	0.05	0.32	0.49	1.26
Japan	0.11	0.16	0.29		
EU major (Fr, Germ, UK)	0.64	0.84	1.07		
All EU	0.93	1.22	1.54	1.62[c]	1.92[c]
Chinese 'diaspora' vs. US 'stayers' (estimate)			0.72[b]		

[a] For 2003 and 2010, ratios calculated using US doctorates at 2001 production level.
[b] 'diaspora' includes estimates of Chinese doctoral graduates from UK, Japan, and US (with temporary visas). US 'stayers' include US citizens and permanent residents.
[c] EU data extrapolated from earlier years.

Table 3: Ratio of foreign STEM PhDs to U.S. STEM PhDs[142]

Of particular concern regarding IT hardware security is the lagging number of students trained in computer security. Information Assurance (IA) programs in the United States graduate only a handful of Master's or PhD students per year. By comparison, one expert suggests that China alone graduates over 30,000 IA students annually.[143] Several initiatives have been launched to address this problem, such as the Federal Cyber Service: Scholarship for Service (SFS). This program allots funds from the National Science Foundation (NSF) to encourage students to enroll in one of 31 institutions that have been designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a "Center of Academic Excellence in Information Assurance" Education (CAE/IAE). The final 10 weeks of study is augmented by an internship

[142] Freeman, Richard B. "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?" NBER Working Paper No. 11457. June 2005.
[143] Personal interview with Information Assurance expert. 29 May 2008.

practicing IA at a federal agency.[144] A second component of the SFS program is capacity building at the participating institutions, where funding is used to assist professional research and infrastructure improvement. For FY2008, the anticipated amount of funds to be distributed is $5.7 million divided among 3-4 scholarships and 10-12 capacity-building awards.[145] Although the objectives of the SFS address the shortage of IA experts in the U.S., the limited amount of funding diminishes the impact of the program.

Aside from the SFS program that aims to educate a civilian core of IA experts, several military institutions of higher learning offer similar programs. For instance, the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD (NII)) distributes scholarship funds to students enrolled in IA programs at various military institutions, including the Air Force Institute of Technology, National Defense University, and the Naval Postgraduate School.[146]

An additional concern aside from the declining absolute numbers of STEM graduates from U.S. institutions is the decreasing ratio of native-born students at American universities. Among engineering disciplines, 49% of graduate students were foreign-born or held temporary student visas in 2002.[147] This trend has significant national security implications, for a large percentage of science and technology graduates from U.S. institutions are unable to receive necessary security clearances. Table 4 illustrates the

---

[144] Federal Cyber Service: Scholarship For Service Information For Students. Oct 2005. 11 Aug 2008. <https://www.sfs.opm.gov/StudentBrochureWeb.pdf>.
[145] National Science Foundation. Federal Cyber Service: Scholarship For Service. 11 Aug 2008. <http://www.nsf.gov/pubs/2008/nsf08522/nsf08522.htm>.
[146] Information Assurance Scholarship Program. 11 Aug 2008. <http://www.defenselink.mil/cio-nii/iasp/>.
[147] Freeman, Richard B. "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?" NBER Working Paper No. 11457. June 2005.

increased number of foreign-born engineering students and decreased number of native-born students in disciplines critical for military R&D.

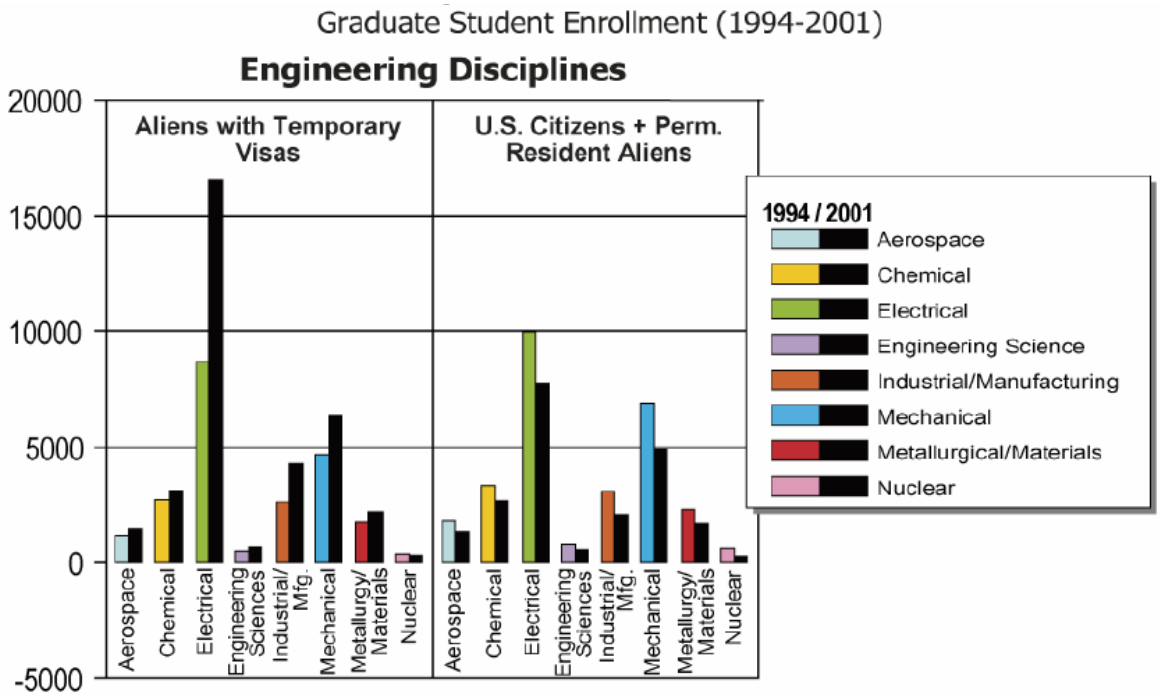

Table 4: University Trends in Defense-Related Science & Engineering[148]

Furthermore, a significant problem that has been recognized from entities such as the U.S. Congress and individuals such as Bill Gates, the founder of Microsoft, concerning career opportunities that do not require security clearances for foreign-born students. Although many foreign students come to the U.S. to attend its world-class programs, many leave after completing their education because of more opportunities abroad. Furthermore, even if a foreign student would like to stay in the U.S. to work, many are

[148] United States. Department of Defense. Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Defense Science Task Force Board On High Performance Microchip Supply. Feb. 2005. 30 May 2008 <http://www.acq.osd.mil/dsb/reports/2005-02-hpms_report_final.pdf>.

denied a work visa or green card, which therefore forces the exportation of intellectual capital away from the U.S. In testimony to the House Committee on Science and Technology in March 2008, Bill Gates stressed not only the importance of increasing funding for and improving the condition of math and science education in the U.S., but also noted the necessity of hiring foreign professionals to staff jobs in the computer science field. The conflicts arise, however, when foreign students cannot stay in the U.S. after the completion of their education. In April 2007, in only two days, the U.S. received over 125,000 petitions for H-1B visas (which allow foreigners to stay in the U.S. to work after completing school), a number that is significantly greater than the 85,000 total cap allotted for that type of visa.[149] Gates accurately sums up the problem when he stated:

> "I believe this country stands at a crossroads. For decades, innovation has been the engine of prosperity in this country. Now, economic progress depends more than ever on innovation. And the potential for technology innovation to improve lives has never been greater. If we do not implement policies like those I have outlined today [H-1B visas], the center of progress will shift to other nations that are more committed to the pursuit of technical excellence. If we make the right choices, the United States can remain the global innovation leader that it is today."[150]

---

[149] McGee, Marianne K. "Bill Gates Says Immigration, Education Reform Needed For U.S. To Compete." Information Week. 12 Mar. 2008. 18 July 2008

[150] McGee, Marianne K.

In short, as the National Science Board's Science and Engineering Indicators 2008 report states, "Educational attainment of the U.S. population has long been among the highest in the world, but other countries are catching up."[151]

Geek Culture

In American culture, there has been a long-held belief of what constitutes a geek or nerd: a scrawny, pale male with no discernable social skills, hunched over his keyboard, playing computer games while compiling some code, perhaps with a pocket protector thrown in for good measure. The reality however, is quite different. Though the term "geek" and "nerd" are often used interchangeably, a geek is someone who is fascinated, and perhaps obsessed, by obscure or very specific areas of knowledge and imagination, whereas a nerd is a person who is perceived to be above-average intelligence and whose encyclopedic interests are not shared by mainstream society.[152] Both fall into a broad category known as "geek culture," but such definitions merely offer a broad categorization of individuals who may belong to the culture without defining the complexities of the culture itself.

Living in an information-driven society, people engage in activity based on information and service instead of industry and agriculture as in the past. The ability to generate and acquire new information is critical, and many in geek culture embrace media technology

[151] National Science Board. Science and Engineering Indicators. Two volumes. Arlington, VA: National Science Foundation (volume 1, NSB 08-01; volume 2, NSB 08-01A).
[152] Konzack, Lars. "Geek Culture: The 3rd Counter-Culture." FNG2006. Preston, England. 15 July 2008.

for work and play and as well as their powerful effects on society. Geeks approach aesthetics and culture differently, seeking substance over ostentation, and want to probe issues for the pursuit of knowledge and experience.[153] Geek culture, then, is best typified by self-selection into communities in which values include many of the traits that have been de-emphasized in the general American culture: intelligence, self-motivation, acumen, learning, synthesis, problem solving, discovery, openness, creativity, and intellectual integrity.

Many of those who categorize themselves as being a part of this group possess the skills, training, knowledge, and education needed to fill the roles in STEM positions for both the government and private industry; however, a cultural barrier exists between those in need of the geek culture skills and those who possess it. In many ways, the government and security communities have had difficulty reaching out to geek culture. As a result, many of America's brightest are left believing that positions in government and security are not available, reachable, lucrative, or respectful of community core values.

There is no question that positions in government and security fields are available; a scan of www.usajobs.gov, the official job site of the U.S. government, using the search term "information assurance" yielded 1,829 available job positions in this field as of August 2008. Other searches with similar terms returned comparable results, a clear indication that such jobs exist. Whether or not these jobs are known to exist by the general public is a separate issue.

---

[153] Konzack, Lars. "Geek Culture: The 3rd Counter-Culture." FNG2006. Preston, England. 15 July 2008.

Although it is obvious that jobs that would appeal to those in geek culture are available, it is also appears as though they are not necessarily attainable. The government operates and communicates on very different channels than those used by geeks; the restrictions placed on secure networks required for government use prevent broad access to and communication with those who operate solely on open networks. While geeks are using social networking sites like Facebook (www.facebook.com) and Twitter (www.twitter.com), as well as blogs and Really Simple Syndication (RSS) feeds (a web feed that is used to publish frequently updated content such as blogs or news headlines)[154], an entire world of communication is being built that operates outside of government missives. When broad agency announcements (BAA) are issued, for example, they are often directed towards private companies and large research universities instead of the public at large. Furthermore, individual agencies issue separate BAAs as needed. A quick search of the term "broad agency announcement" returns many results for individual BAAs issued by agencies, however, no topical compilation exists to allow for easy searches that locate and isolate relevant proposals for research. One can narrow the field by using the search parameters "broad agency announcement" plus the specific field of interest, but in order to be successful with this method, one must first be aware of BAAs, and then must be cognizant of what key search terms would be necessary to tighten the parameters to produce the desired results.

---

[154] RSS Advisory Board. "RSS 2.0 Specification." RSS Advisory Board. 18 Aug. 2008 <http://www.rssboard.org/rss-specification>.

Additionally, if one is able to locate a job that would fit his or her skill set on www.usajobs.gov, for example, the complicated and convoluted qualifications and evaluations requirements make the process of obtaining a government job difficult Furthermore, obtaining a government job without prior specialized government experience seems unlikely. This seemingly preferential treatment for current government or military employees or veterans could dissuade non-government individuals from even attempting to apply when it appears doubtful they would be hired. Furthermore, many of the jobs in these areas of expertise require a security clearance, which most citizens do not have. In order to obtain a position in information security, one must have a security clearance, but one cannot obtain a clearance until one has had a job in which a clearance was acquired. This establishes a "chicken or egg" problem that many are not able or willing to try to resolve. As a result, the pool of legitimate talent in many areas is greatly reduced for government employment.

Although money is not necessarily the primary motivator for many geeks, it is still an important aspect of one's career. Continuing with the www.usajobs.com example of an information assurance specialist position, the starting salary provided on the website was $25,623.00,[155] and the salary was dependent on both experience and location. Comparably, the average salary of an information security specialist in private industry

[155] "Information Assurance Specialist." USA Jobs. 07 Dec. 2007. 07 Aug. 2008 <http://jobsearch.usajobs.gov/getjob.asp?jobid=66135396&brd=3876&avsdm=2008%2d06%2d26+21%3a56%3a34&sort=rv&vw=d&q=%22information+assurance%22&logo=0&ss=0&customapplicant=15513%2c15514%2c15515%2c15669%2c15523%2c15512%2c15516%2c45575&tabnum=1&rc=5>.

averaged $78,357.00.[156] With industry standards being almost three times the government beginning wages, performing the same job for less money makes little sense. Additionally, it could take several months to be cleared to work in a government position if one has never worked for the government or military before. Therefore, in addition to complicated hiring practices, lower salaries may prevent many of those with the skills to contribute to the governments' network security from seeing any incentive in accepting a government position.

Finally, respect of core values is critical for incentivizing individuals in the geek culture to work in government positions. Although many of the military services' core values do not conflict with the values highlighted in geek culture, several have the potential to do so. In particular, both the Air Force and the Army value "service before self" and "selfless service," which asks individuals to put the welfare of America, the service, and others before oneself.[157] [158] The "self" is an idea the geek can understand; the self is a realistic concept that can be studied, dissected, and ultimately understood. A geek knows him or herself well, understanding why he or she acts a certain way, is or is not attracted to something, or gravitates towards a certain job. What is less clear is "service;" this terms begs many questions such as "service to whom? what service is necessary? to what end? why? how will this research or work be used?" This idea is more notional since it is likely that a geek will not be able or allowed to understand the complete operational

---

[156] "2007 Salary Survey: Staff and Entry-level Positions." Computerworld. 18 Aug. 2008 <http://www.computerworld.com/spring/salary-survey.htm?activeyear=2007&type=job_levelmeter=0&page=1>.
[157] Donley, Michael B. "Letter to Airmen." 13 Feb. 2006. 19 Aug. 2008 <http://www.af.mil/library/viewpoints/secaf.asp?id=217>.
[158] The Seven Army Values." 10 Oct. 2003. 19 Aug. 2008 <http://www.history.army.mil/lc/the%20mission/the_seven_army_values.htm>.

structure of the entity requiring the service. It makes little sense then, to a geek, to devote one's life, or self, to something that essentially is a black box, something considered to be mysterious about which we do not or cannot understand its inner workings, and only have access to its inputs and outputs.[159] A geek will choose the concrete "self" instead of the notion of "service" that creates many potentially unanswerable questions.

Furthermore, creativity is a prime motivator for geeks in various professions. The possibility of introducing new ideas, improving upon existing ones, and creating new methods of information and idea exchange is a central characteristic to geek culture.[160] A problem exists, however, in the perception of those in geek culture and academia that the military and government resort to the same tactics from the past to solve current problems and are unwilling to allow creativity and innovation to flourish. It should be noted, however, that creativity is vital to the sustainability of the military. In order to ensure rapid and secure maintenance and strength of forces across a wide array of military operations throughout the world, those in charge of sustainment must be "creative masters of transition" to be able to predict and overcome potentially monumental and time-sensitive issues.[161] Former Secretary of Defense Donald Rumsfeld recognized the necessity of fostering environments of creativity and innovation in both military and government institutions:

---

[159] "Origin of the Term "Black Box"" Google Answers. 2002. 19 Aug. 2008 <http://answers.google.com/answers/threadview?id=114741>.
[160]Konzack, Lars. "Geek Culture: The 3rd Counter-Culture." FNG2006. Preston, England. 15 July 2008.
[161] Colonel Harman, Larry D. "Creativity: The Sustainer's Field of Dreams." U.S. Army Logistics Management College. 19 Aug. 2008 <http://www.almc.army.mil/alog/issues/marapr03/ms864.htm>.

> "But we need to transform not only our armed forces, but also the Department of Defense itself, by encouraging a culture of creativity and sensible risk taking. We need to encourage a more entrepreneurial approach to developing military capabilities -- one that is not mired in the past and one that does not simply wait for new threats to emerge to take us by surprise."[162]

Several companies have taken the need for innovation and creativity to heart. For example, Google Inc. instituted an "80/20" rule, where their employees work on core projects as laid out in their job descriptions 80% of the time; the remaining 20% of their time can be used to pursue whatever interests them, whether it's creating new products or applications for Google or fixing an existing one.[163] Not only does this policy increase productivity during 80% time when employees are focused on tasks directly related to their jobs, but it also directly benefits the company in other ways. In late 2005, 50% of what Google launched in terms of new applications and features came from 20% time.[164] Marissa Mayer, Vice President of Search Product and User Experience at Google, explains this explosion of productivity as stemming from the passion and momentum employees maintained while pursuing their own interests in search of innovation and creativity. If a company or agency trusts its employees, and wants to encourage creativity and expansion, then employees will want to pursue projects that both satisfy their need for creativity and benefit the company or agency as well.[165]

---

[162] Rumsfeld, Donald H. "U.S. Joint Forces Command Change-of-Command Ceremony." U.S. Joint Forces Command Change-of-Command Ceremony. Norfolk, VA. Defense Link. 02 Oct. 2008. 19 Aug. 2008
[163] Mayer, Marissa. "9 Notions of Innovation." Stanford University, Palo Alto, CA. 19 Aug. 2008.
[164] Mayer, Marissa.
[165] Mayer, Marissa.

Finally, an important core value present in geek culture is symptomatic of a culture devoted to open exchange.[166] The idea of openness is intrinsic among geek culture. Several movements have swept throughout this sub-culture and across the internet concerning open source materials such as software, journalism, and knowledge, as well as innovative sharing practices that branch out from traditional copyrights among authors, scientists, artists, and educators to allow for the free exchange of ideas and products while still retaining one's rights. The open source movement initially focused predominantly on software with the belief that the more eyes that looked at a program to isolate its bugs and operating errors the more secure, operational, and stable the program would be.[167] Furthermore, the Creative Commons movement provides free tools that let authors, scientists, artists, and educators easily mark their creative work with the freedoms they want it to carry, ranging from "All Rights Reserved" to "Some Rights Reserved."[168] Much like the free software and open-source movement, the goals of Creative Commons are cooperative and community-minded in that they aim to not only increase the amount of raw material open to consumption that is on the internet, but also make access to that material cheaper and easier.[169] Geeks gravitate to such movements and ideas because they are seen as reductions in barriers to creativity, allowing them to share, sample, and create without fear of legal action.

---

[166] Konzack, Lars. "Geek Culture: The 3rd Counter-Culture." FNG2006. Preston, England. 15 July 2008.
[167] Poynder, Richard. "The Open Source Movement." Information Today. Oct. 2001. 19 Aug. 2008 <http://www.infotoday.com/it/oct01/poynder.htm>.
[168] "Creative Commons." Creative Commons. 19 Aug. 2008 <http://creativecommons.org/>.
[169] "History." Creative Commons. 13 July 2007. 19 Aug. 2008 <http://wiki.creativecommons.org/history>.

This, however, establishes an interesting dichotomy in that the government often does, and sometimes absolutely must, operate within a realm of secrecy. In times of war, threat, or danger, the ability of the military or government to control what information is out for the world to see is critical. The necessity for secrecy and the desire for openness do conflict at high levels, and this rift could help explain the difficulties the government and military have had reaching out to geek culture.

RECOMMENDATIONS

In order to achieve solutions that address the problem from a holistic approach with both short term and long term goals in mind, policy support and technological methods must be employed in combination to ensure security of foreign-manufactured IT hardware. Below, policy recommendations and technological solutions are presented, and when implemented together, could address the major issues associated with using IT hardware in critical systems that was created in an untrusted environment.

Policy Support and Solutions

To address the vulnerabilities associated with subversion and counterfeiting of foreign sourced IT hardware, a range of policy reforms and initiatives are recommended. Two classes of policy recommendations are presented: the first class aims to ensure the availability of a secure supply, while the second seeks to improve intellectual assets present, though perhaps underdeveloped, in the United States.

Controlling Hardware Supplies

Eliminating the threat completely from subverted or counterfeit hardware is implausible if not impossible; if the motive exists, the act will likely occur. Thus, ensuring that legitimate, clean hardware is acquired and installed into critical networks is essential. Below are policies whose objectives are to control the supply of IT hardware. These

include providing economic incentives for IT firms, expanding trusted foundry programs, and restructuring import and acquisition regulations.

Economic Incentives for Domestic Design

Markets typically provide sufficient incentives to address security issues, yet this has not always proven to be the case with respect to cyber security. As a result of market failures, several proposals have been offered that would ensure markets produce effective, innovative responses to security vulnerabilities, but require limited government intervention.

It is recommended that the government provide subsidies or capital grants to direct the market towards greater security measures. This is consistent with the case studies discussed in Appendix B (page 119) where IT firms were attracted to China and Ireland in part because of economic incentives, such as tax breaks, granted by the state.

Additionally, an important development is the passing of legislation currently in the 110th Congress that would permanently extend the R&D tax credit. This credit was first implemented in 1981 and has been temporarily extended multiple times since its passage. Although the pieces of legislation in the House of Representatives (H.R. 2138) and Senate (S. 2209) will have to be reconciled, the core objectives are the same: extend R&D tax credits to maintain America's research competitiveness.[170]

[170] See Appendix C: Tax Credit Bills (page 123). H.R. 2138 and S. 2209. 2006-2008. 05 Aug 2008. <washingtonwatch.com>.2006-2008. 05 Aug 2008. <washingtonwatch.com>.

State governments can also provide tax credits for R&D activities that would provide incentives to companies engaged in R&D. As of 2005, 31 states offered such incentives. These tax credits largely replicate the federal model, and have become increasingly generous over time.[171] Although these credits – both federal and state - apply to all industries, these are particularly important for the IT industry. Productivity growth in the whole economy, as noted earlier, is greatly affected by innovations which emanate from the IT industry.

Combined federal and state tax credits offer U.S. firms incentives to maintain their domestic R&D activities. To encourage the growth of innovative ecosystems (geographic collocation of R&D and manufacturing), tax credits for manufacturing should also be extended.

In addition to tax credits and capital grants, the U.S. government can communicate to IT firms the various advantages associated with domestic R&D and manufacturing. As the analysis presented in Appendix A suggests, IT firms do not necessarily prioritize intellectual property rights, political freedoms, or economic non-interference in comparison to other factors. The United States, in contrast to some states that are currently attracting large inflows of IT FDI, offers an environment where IP rights are strictly protected, civil unrest has little chance of disrupting operations, a skilled workforce exists, and limited state intervention in business.

---

[171] Wilson, Daniel. "The Rise and Spread of State R&D Tax Credits." FRBSF Economic Letter 2005-26. 07 Aug 2008. <http://www.frbsf.org/publications/economics/letter/2005/el2005-26.pdf>.

Trusted Foundries

The NSA's Trusted Access Program Office (TAPO) was assigned by the government to find and maintain trusted suppliers to ensure that the government and intelligence community can receive critical components for critical and secure networks. TAPO has arranged for the Defense Microelectronics Activity group to certify trusted suppliers. As of July 2008, more than a dozen corporations have been accredited as trusted suppliers.[172]

Since technological methods for confronting the threat of hardware subversion are currently being researched, refined, and implemented, expansion of and increased funding for trusted foundry programs is essential. Trusted supplier or foundry programs have had success in the manufacturing phase; however, in order for a foundry to be completely trusted, all phases of the supply chain need to be secured.[173] The handling and shipping phase is often performed in an untrusted environment, and opens a window of opportunity for potential tampering.

Therefore, it is recommended that the existing trusted hardware programs be extended to include all phases of the supply chain, especially the shipping and handling phase. Recognizing that this may not be feasible, new programs that allow for trusted domestic handling and shipping must be developed.

---

[172] Defense Microelectronic Activity. "Trusted IC Supplier Accreditation Program." July 2008. <http://www.dmea.osd.mil/docs/AccreditatedSuppliers.pdf>

[173] Tech Talk. "Trust in Integrated Circuits." June 2008.

Import & Acquisition Regulations

Though subject to a different set of policies and laws, the U.S. pharmaceutical import regulations provide ideas for best practices regarding IT imports.

Even though the wide-scale implementation and security of RFID technology is still under investigation, requiring a "pedigree" that details every step of the IT product's path from its inception to its final destination would help ensure the validity of the product. A pedigree represents the complete history of a product's chain of custody from the manufacturer to the point of dispensing.[174] Like Florida's 2006 expanded requirements for paper-based pharmaceutical pedigrees, such a program allows for electronic verification of pedigrees, currently through barcodes, but potentially in the future through RFID.[175] Expanding this practice to IT imports, the U.S. should require complete pedigrees for foreign-manufactured IT components, especially those that could be installed in critical networks, such as government or security/intelligence community networks. Though not a silver bullet, requiring such thorough documentation for critical components helps keep the critical networks in the U.S. secure from faulty products or malicious intentions.

Just as the Food, Drug, and Cosmetic Act covers specific items for import, additional regulations should be enacted specifically for IT products. Since many of the IT components used in commercial and governmental networks are produced overseas, extra

---

[174] "Beyond Pedigree: The Role of Infrastructure in the Pharmaceutical Supply Chain." Verisign. 7 July 2005. 6 Aug. 2008 <http://www.verisign.com/static/031078.pdf>.
[175] Faber, Paul. "RFID Strategy -- Pharmaceutical E-Pedigrees and RFID." IndustryWeek. 16 Oct. 2007. 12 July 2008 <http://www.industryweek.com/readarticle.aspx?articleid=15180>.

security measures to ensure their validity and security are essential. As mentioned in the technology overview (page 8), testing ICs is time consuming, cost-ineffective, and next to impossible to do. Testing several chips per batch, however, could provide extra security measures to identifying at least counterfeit products.

Finally, since one of the main incentives for counterfeiting products is the extensive economic gain,[176] implementing harsher penalties for counterfeiters could provide a disincentive to producing, ordering, or importing counterfeit products. As discussed on page 2, Cisco Systems was the target of a large-scale counterfeit scam in 2007, with false products being placed in critical systems such the FBI, the Marine Corps, the Air Force, the Federal Aviation Administration, defense contractors, universities, and financial institutions. Of the men convicted of fraud and counterfeiting, the most that anyone had to pay back in restitution was approximately one-third the amount of counterfeit product sold; the longest prison sentence was approximately 5 years.[177] Increasing the potential costs of selling or producing counterfeit products, especially to agencies and/or companies whose breach could impact national security, could dissuade potential counterfeiters from importing and/or selling counterfeit products in the U.S. This, in turn, could reduce the chance that faulty products ending up in critical U.S. networks and systems.

---

[176] "Product counterfeiting." Global Legal Information Network. Library of Congress. 31 July 2008 <http://www.glin.gov/subjecttermindex.action>.
[177] Rybicki, Jim. Departments of Justice and Homeland Security Announce International Initiative Against Traffickers In Counterfeit Network Hardware (Press Release). Federal Bureau of Investigation. Washington Field Division. 2008.

In addition to import regulations, acquisition policies could provide an essential component of a strategy to alleviate hardware subversion threats. Due to the complex nature of acquisition regulations and their continuously evolving nature, these policies should be streamlined in order to facilitate universal implementation. Additionally, DoD acquisition policies concerning IT products should be designed from a security perspective rather than from a price-only viewpoint.

Furthermore, the newly enacted exception to the Berry Amendment is a positive development; this decision-making flexibility should be exercised to its fullest extent, especially with respect to IT hardware in critical networks.

Longevity of Trust-Based Solutions

Though programs based on trust are valuable, they cannot provide the foundation for long term solutions to this ever-growing problem. Some industry experts have remarked that no matter how secure or how trusted the foundry may be at the moment, the reality is that these programs are not enough to solve the problem. Thomas Hartwick, chairman on the DoD Advisory Group on Electron Devices, noted that, "special arrangements with domestic chip manufactures are a band-aid solution that our government has put in place for the time being." Many in the industry suggest that the only effective, long term solution to this problem is to reemphasize the domestic manufacturing base. Hartwick recommended a "long term national strategy to reverse the offshore trend," and "immediate government action," be taken. Even the private sector of the IT industry has taken note of this possibility. IBM's Technology Division's Vice President of Strategic

Alliances noted that the domestic semiconductor industry is, “at risk,” and that “the U.S. needs a new semiconductor partnership strategy plan.” He acutely summarized the situation by adding that “the resulting diminution of U.S. semiconductor manufacturing base has many implications including the U.S. government’s inability to obtain needed chips reliably.”[178] It should be clear, then, that the U.S. cannot base the solution to this issue solely on our ability to trust a select set of manufacturers here or abroad. However, there are initiatives that can provide the U.S. with an edge regarding the development of our own intellectual assets, as elucidated below.

Developing Intellectual Assets

The United States became the leader in scientific discovery in part because of the vast wealth of intellectual assets it possesses. Yet, as discussed previously, these assets are not being fully developed or utilized. Improving the education system and refocusing on the importance of math and science is critical if the U.S. is to maintain its technological edge. Furthermore, current assets are not being exploited; the disconnect between government and geek culture deprives the U.S. of the talents of many gifted individuals.

Education Initiatives

Several of the proposed recommendations below should not require great amounts of additional funding, but rather a refocusing of time, energy, and already available assets to

[178] McCormack, Richard. "Manufacturing & Technology News." 3 February 2004. Volume 11, No.3. June 2008. <http://www.manufacturingnews.com/news/04/0203/art1.html>

promote further knowledge and interest in math and science fields. Additionally, it will be imperative to spark a child's interest early in childhood, not wait until high school to promote the possible careers related to math and science.

Child care centers offer a prime example of the possibility of targeting young children. Young children learn very well through hands-on activities, and conducting simple experiments allows them to see that science and math can be fun. Experiments such as the "mini ocean" experiment, the "raising raisins" experiment, and the "invisible ink" experiment are simple, safe, and cost-effective methods from which young children can learn the basics of scientific principles, ideally encouraging them to pursue such interests later in life.[179] More difficult experiments are readily available for older children that are also equally cost-effective. Creating crystals with borax, water, and food coloring, and conducting cornstarch suspension (mixing cornstarch and water that is a solid when manipulated and a liquid when resting) allow older children to explore more advanced concepts such as suspension, evaporation, and differences between liquids and solids.[180] Such methods would be especially advantageous in before- and- after-school programs, and would require little funding to conduct. The return, in the form of interested and engaged students, should outweigh the costs.

---

[179] "Preschool Science Fun and Experiments." Child Care Lounge. 1 Aug. 2008 <http://www.childcarelounge.com/caregivers/sciencefun.htm>.
[180] Fitzpatrick, Diane L. "Simple Science Experiments: Young Children Can Do Easy, Fun Science Projects At Home." Suite101. 8 Oct. 2007. 1 Aug. 2008 <http://parent-child-activities.suite101.com/article.cfm/simple_science_experiments>.

More specifically, encouraging math and science among programs in schools for "high-ability learners," or children deemed "gifted and talented," would do much to spark interest in the fields at an early age. High-ability learners are marked by their distinctive blend of abilities and talents, as well as rates and styles of learning. Such students are often typified by characteristics such as high performance rates in intellectual, creative or artistic endeavors when compared to other children in similar age groups or environments, which would require services or activities not ordinarily provided by the schools to foster and develop such skills.[181] Activities involving math, science, and computers would coincide well with the advanced teachings that high-ability learners receive, and hands-on experiments and field trips (to local university science departments, for example), would allow students to observe the practical application of the content they learn in school.

Furthermore, additional funding should be allocated to establish more science and math summer camps for older children and young teens. A good example is the University of Nebraska-Omaha Physics Department and NASA's collaborated "Aim for the Stars" science camp that is offered every summer. Children from fourth to eighth grade have opportunities to attend different camps, which are separated by age groups, and specific camps for girls are offered as well.[182] Some of the weekly sessions that are offered through this include astronomy, energy alternatives, strategies of the mind, and TEKBOT and ROBOLAB, in which children learn about the basic applications in wireless, video,

---

[181] Cognard, Anne, Robert Bednar, Bill Roweton, Noreen Ward, Linda Wells, and Deanna Zweifel. Procedures for the Identification of High-Ability Learners. Nebraska Department of Education. Lincoln: State of Nebraska, 1997.
[182] University of Nebraska at Omaha. Aim for the Stars. 2005. 18 July 2008. <http://www.unomaha.edu/aimforthestars/>

and signal processing, sensors, electronics, control system, as well as the fundamentals of programming. Programs like these are invaluable for their ability to instill interest and foundational skills necessary for succeeding in these areas of interest later in life.[183] In addition to increasing funding for additional similar programs, more scholarships should be offered to attract economically-disadvantaged students.

It is also recommended that computer programming and advanced computer training be introduced at a younger age through expanded funding for developing and implementing computer programming education. Though students entering college may originally be interested in a computer science or computer engineering degree, many who do not have any prior experience or knowledge concerning computer programming are easily frustrated by the very different skill set and logic-based thought processes required to succeed in such majors. A nationwide survey conducted by the Higher Education Research Institute at UCLA showed that incoming computer science majors declined more than 60 percent from 2000 to 2004. Among female students, interest in computer science declined 80 percent between 1998 and 2004.[184] Researchers at Carnegie Mellon developed the Alice Initiative to combat such trends. Instead of trying to decipher pages and pages of code, this program allows students to learn fundamental programming concepts by creating animated movies and simple video games through dragging and dropping commands to create a program where the instructions correspond to standard

---

[183] University of Nebraska at Omaha. "Complete List of Camps." Aim for the Stars. 2005. 18 July 2008 <http://www.unomaha.edu/aimforthestars/pages/allcamps.php>.
[184] "Alice: A Wonderland." Carnegie Mellon. 1 Aug. 2008 <http://www.cmu.edu/homepage/practical/2007/fall/alice-a-wonderland.shtml>.

statements in a production oriented programming language such as Java, C++, and C#.[185] Using this method, students can instantly see how their commands will execute through animating 3-D avatars, which enables them to understand the relationship between the programming statements they enter and the behavior of objects in their program.[186] This program is available for middle- and high school students, allowing more time for the interest to develop before entering higher education. Programs like this are vital to reaching out to younger generations of potential computer scientists and other populations that have generally avoided this area of study, particularly women.[187]

Renewing the interest in STEM areas of study is critical for America to remain competitive on a global stage of technology. Working in combination with the curriculum designed at the state and district levels, many of these recommendations are simple, low-cost methods for engaging students with hands-on, real-world experiments that allow them to see the usefulness and creativity inherent in math and science.

Several options are also available to address the declining emphasis on and interest in STEM disciplines in institutions of higher education. A readily implementable solution to the problem concerning the loss of intellectual capital would be to raise the number of H-1B visas and worker-green cards allowed each year. As shown in the higher education overview (page 45), demand far outstrips supply, and allowing more foreign students to remain in the U.S. to work for U.S.-based companies to contribute to technological

---

[185] "Alice: A Wonderland." Carnegie Mellon. 1 Aug. 2008 <http://www.cmu.edu/homepage/practical/2007/fall/alice-a-wonderland.shtml>.
[186] "Alice: A Wonderland."
[187] "Alice.org." What is Alice? 28 July 2008 <http://www.alice.org/index.php?page=what_is_alice/what_is_alice>.

innovation until U.S. professionals can fill in the gaps created by low domestic engineering levels. Several bills are currently awaiting a final decision from Congress to address the current shortfalls associated with the issuance of H-1B visas. Of particular note is H.R. 5630, or the Innovation and Employment Act. Significant proposals within H.R. 5630 are to:

- Double the amount of H-B1 visas to 130,000 starting in FY2008
- Exempt from H-1B visa caps any alien who has earned a Master's or PhD STEM degree from a U.S. institution of higher learning if an employer requires such education[188]

Additionally, the decline in federal funding for scientific research is a perceived sign that such professions offer little chance for success or value. Increasing the amount of funding available for scientific research would generate more interest in the fields as well as additional innovation in STEM professions. The American Competitiveness Initiative (ACI), launched by President Bush in 2006, is a worthy endeavor toward this goal. One of the stated objectives of the ACI is to double the amount of funds allocated for research centers such as the NSF, the Department of Energy's Office of Science, and the Department of Commerce's National Institute of Standards and Technology over 10 years. Additionally, the ACI intended to improve STEM programs at colleges and universities throughout the country.[189] The ACI is a valuable undertaking to increasing funding for research centers; however, the lack of funding has thus far prevented this

[188] The Library of Congress, Bills and Resolutions. 07 Aug 2008. <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.5630>.
[189] Domestic Policy Council Office of Science and Technology Policy. American Competitive Initiative. Feb 2006. 15 Aug 2008. <http://www.whitehouse.gov/stateoftheunion/2006/aci/aci06-booklet.pdf>.

initiative from achieving its goals. Allotting funding for this initiative will aid in basic research funding so that America can remain competitive.

Furthermore, it is recommended that the number of scholarships awarded through the NSF's Federal Cyber Service: Scholarship for Service should be increased from the 3-4 currently allotted for FY2008. The expansion of this scholarship program will help train a force of cyber experts knowledgeable of and interested in federal government work. Funding for research centers should be granted to keep pace with the original goal of doubling the funds over 10 years.

Another method to attract interest in STEM disciplines at the university level is to promote private-sector participation. For example, students at the Entertainment Technology Center at Carnegie Mellon collaborate with firms in their research of cutting-edge entertainment technologies. Through the partnership with companies such as Walt Disney, Electronic Arts, and Microsoft, students become acclimated with the real-world application of current generation technologies.[190] In addition to partnering with universities, companies have developed programs intended to train and recruit its future workforce. Participants in ExxonMobil's Pre-Employment Programme are awarded scholarship funds, assigned a mentor, and tasked with projects relevant to the company's operations.[191] Through such private-sector programs, students are educated not only in a

[190] "Entertainment Technology Center." Carnegie Mellon. 15 Aug 2008. <http://www.etc.cmu.edu/index.html>.
[191] "Pre-Employment Programme." ExxonMobil. 15 Aug 2008. <http://www.exxonmobil.com.sg/AP-English/Jobs/SG_Work_preemployment.asp>.

STEM discipline, but also about what employment opportunities are available following graduation.

Geek Culture Outreach

Several recommendations are available to increase the contact and communication between geek culture and the government. It is important to note that while these recommendations also do not necessarily require a significant amount of funding, policy changes may be necessary to implement such recommendations with the government.

First, it is highly recommended that the government use open channels of communication to reach out to those in geek culture. This recommendation would not only be easy to implement in a short time frame, but also cheap, since no incremental monetary adjustments are necessary except for the cost of personnel who would fulfill these outreach projects. Websites like Twitter, Facebook, or LinkedIn, blogs, and RSS feeds, as well as attendance at geek events such as BarCamp (an ad-hoc gathering born from the desire for people to share and learn in an open environment that focuses on many different topics)[192] are quick and easy ways of reaching a large portion of the geek culture. Though information disseminated through such methods would need to be screened, using such channels is beneficial because it will show the geek culture that the government and military are willing to step outside their realm of secrecy and communicate with geeks at the geek level. This would foster trust and willingness to work with the government if it is perceived as being willing to work with geeks.

---

[192] "BarCamp Wiki." BarCamp. 20 Aug. 2008 <http://barcamp.org/>.

Furthermore, if such outreach practices are employed, implementers should be careful to observe the colloquial and conversational style of the medium to ensure that they appropriately engage the community. It is highly recommended that government employees who perform the task of engaging the geek community are upfront with whom they are and what their aims are, but do so in a fashion that does not convey BAA-style rhetoric, which is too institutional and potentially off-putting.

Next, it has been shown that creativity is key to both geek culture and the military and government. To deconstruct the belief widely held in geek culture and academia that the military and government do not care and do not encourage creative ideas, it would be advantageous for the government to provide more creative autonomy within the job description so that as long as the work is completed, the geeks can achieve that goal in whichever manner suits them best. Though the geek will still be completing the task as hand, he or she is doing it in a manner which would satisfy his or her need for understanding and the need to draw his or her own conclusion from the information at hand. This would not require significant funding, but would require a shift in policy and culture.

Finally, it is recommended that a pilot program be implemented to test the validity of a program like Google Inc.'s "80/20" rule. It is recommended only as a pilot program because of the obvious differences between Google Inc. as a private company and the government, which pays its employees with tax-payer money. To establish this program initially with only a small group would allow the government to demonstrate to the general public that the return during the 80% time could be higher than without the

rule during 100% time, much like what Google Inc. has experienced since implementing this program. Furthermore, during 20% time, employees could use this time to improve upon existing ideas, research possible future courses of action, or innovate and create ideas that would directly benefit the US.

Technological Methods and Solutions

While policy provides an essential component of a strategy to thwart potential counterfeiting and subversion of hardware for critical systems and networks, technology developments often move faster than policy. Adaptive technological solutions will be required in addition to the policy solutions outlined if hardware subversion and counterfeiting are to be secured sufficiently.

As discussed in the technological overview (pg. 8), functional verification works as a quality control measure, and should persist for that purpose. It cannot, however, provide security against malicious hardware inclusions and counterfeit hardware. Several other methods show promise for this purpose, including an alternate type of verification, proactive design of security elements into ICs, tracking measures through acquisition and shipping processes, and measures exercised cooperatively with manufacturers.

Side-Channel Verification

An alternative to functional verification is side-channel verification, which works by examining circuit parameters. The concept of side-channel verification simply means that side-channel parameters of chips, rather than functional aspects, are measured and

examined. A number of specific side-channel verification methods have been studied and developed over recent years. In 2007, researchers at IBM's T.J. Watson Research Center and the Worcester Polytechnic Institute outlined a method by which side-channel verification might be employed. The steps included:

1. Selection of random ICs from a single "family" (shared design mask and fab, or fabrication facility).

2. Sufficient input/output (I/O) tests to exercise expected circuitry, and collection of side-channel data through the course of these tests. (Because these tests are only designed to exercise expected circuitry rather than exhaustively trigger all possible conditions, this testing is feasible within limited time-frames – in fact, this stage could re-use test patterns from functional verification quality control steps, which are designed to provide minimal I/O to sufficiently exercise circuitry.)

3. Development of a "side-channel fingerprint" from these data.

4. Destructive testing of selected ICs by using techniques like demasking, delayering, and comparison to X-ray scans of layers with masks – essentially, disassembling the chip and comparing it to the blueprints.

5. Testing of all other chips in the family by comparison of side-channel fingerprints with those generated from the original test batch. This last step should only be executed if the chips in the test batch were verified as manufactured to specification during step four.[193]

[193] Agrawal, Dakshi, Selçuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. "Trojan Detection using IC Fingerprinting." IBM T.J. Watson Research Center and Worcester Polytechnic Institute, 2007 IEEE Symposium on Security and Privacy (SP'07), 20-23 May 2007, Berkeley, CA, USA.

This procedure is significant in that it does not require trusted fabrication – subversion attempts by a manufacturer would be revealed at step four, when test batch chips failed to pass the manufactured-to-specification challenge. It does, however, require trusted design; if subversive features were present in IC specifications, there would be no "gold standard" with which to compare chips. The reverse engineering performed in the fourth step is time-consuming and expensive, taking up to a week and $250,000 to destructively test a single chip.[194] However, because only a small percentage of chips would be subject to this process, the cost would be significantly reduced over the entire chip family. The IBM-WPI team developed side-channel fingerprints using power analysis and this process. In their experiment set, they were able to easily identify all chips containing trojans down to 0.12% of the total circuit size. Further statistical analysis on power distributions allowed the team to identify all trojans down to 0.01% of the total circuit size with one circuit falsely identified (a 2% false positive rate).[195] A team of researchers at University of Illinois at Urbana Champaign (UIUC) recently designed and implemented a hardware trojan. In their research, they suggest that a 0.05% to 0.08% increase in circuit logic is likely to be the smallest trojan that could give arbitrary access using their method (allowing unprivileged malicious software to access privileged memory regions on the chip), regardless of the overall size of the chip.[196]

---

[194] King, Samuel T, et al. "Designing and Implementing Malicious Hardware." University of Illinois (2006).
[195] Agrawal, Dakshi, Selçuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. "Trojan Detection using IC Fingerprinting." IBM T.J. Watson Research Center and Worcester Polytechnic Institute, 2007 IEEE Symposium on Security and Privacy (SP'07), 20-23 May 2007, Berkeley, CA, USA.
[196] King, Samuel T, et al.

The UIUC researchers also suggest, however, that trojan detection via the methods used by the IBM-WPI team may not be as easy as experimental results imply. Power analysis methods, they explain, originated as an attack technique, which means that there is a large body of research concerning methods for preventing its use. For someone implementing trojan circuitry, these countermeasures would be particularly feasible, because it would only be necessary to implement them for a small subset of the chip.[197] These factors may be possible to counteract by using an alternate parameter for developing fingerprints[198] or by analyzing parameters across smaller regions of a chip to reveal small or obfuscated trojans.[199] Research that emphasized combining several of these strategies would be ideal.

Physical Unclonable Functions (PUFs)

The adage that a ounce of prevention is worth a pound of cure is as true in hardware security as in any other field, so it is appropriate that recommended methods for securing hardware include at least one preventative measure. In a sense, encapsulation (the coating of circuitry with resins) is a preventative subversion countermeasure, because it makes subversion difficult. A more robust preventative solution involves designing and integrating Physical Unclonable Functions (PUFs) into chips. PUFs are:

- Physical in that they are based on properties of the physical circuitry

[197] King, Samuel T, et al. "Designing and Implementing Malicious Hardware." University of Illinois (2006).
[198] Jin, Yier, and Yiorgos Makris. "Hardware Trojan Detection Using Path Delay Fingerprint." Yale University, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08), 9 June 2008, Anaheim, CA.
[199] Banga, Mainak, and Michael S. Hsiao. "A Region Based Approach for the Identification of Hardware Trojans." Virginia Polytechnic Institute, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08), 9 June 2008, Anaheim, CA.

- Unclonable in that they are easily evaluated on-chip in a finite amount of time, but difficult for an attacker to characterize without unlimited time and resources

- Functions in that they map challenges to responses, meaning they exercise the circuit in some way (the challenge) and receive some value or set of values back (the response)

A few extra criteria provide strength to the solution for the purposes of securing hardware, and are met by integrating PUFs directly into the silicon of an IC:

- A PUF is manufacturer resistant if it is technically impossible to produce two identical PUFs given finite time and resources. A silicon-integrated PUF would measure the side-channel effects of tiny variations from chip to chip that cannot be removed by the manufacturing process (in fact, these variations are inherent to the manufacturing process). A manufacturer could not create two chips which returned identical values from PUF challenges.

- A PUF is controlled if it can only be accessed by a mechanism that is physically inseparable from the PUF.[200]

The ideal, then, is a manufacturer resistant, controlled PUF. The integration of this sort of PUF into an IC would effectively make the IC self-aware in the diagnostic sense; the chip itself would test to ensure that it was valid. Singly, none of the manufacturing variations that provide this security mechanism would provide unique identification, but in combination, many variations become an identity, much as the many whorls and loops on a finger combine into a unique fingerprint.

---

[200] Gassend, Blaise, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. "Silicon Physical Random Functions." Massachusetts Institute of Technology, Conference on Computer and Communications Security 2002, 18-22 Nov. 2002, Washington, D.C. Proceedings of the 9th ACM conference on Computer and communications security. Washington, D.C.: ACM, 2002.

To provide unique identification for one billion ICs, it is estimated that a minimum of 60 bits of information would be required, which would require sufficient PUF elements to provide between 40 and 90 challenges (the higher number accounting for fluctuations in responses due to greater changes in operating temperature of the circuit). Each order of magnitude increase in the number of ICs to be uniquely identified should result in only a linear requirement in the increase of PUF elements; in other words, going from 1 billion ICs to 10 billion ICs should only require 6-10 more PUF elements. This reverses a typical trend in which technology that is more ubiquitous is more difficult to secure.[201]

In order for the unique identification provided by PUFs to help verify foreign hardware, PUFs must be registered post-manufacture with a domestic database. Then, immediately before install, PUFs can be checked against this database to verify that they are the expected chips rather than counterfeit versions that have not been subject to side-channel verification.

Radio Frequency Identification (RFID) and Tracking

Radio Frequency Identification (RFID) provides a potential third leg of a strategy to secure the supply of ICs through technological means. RFID chips are designed to provide a unique identification for an item which can be read and verified by emission of radio waves rather than line-of-sight access to the item. Original applications of these chips focused in particular on eliminating UPC and other sorts of barcodes (which require

[201] Gassend, Blaise, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. "Delay-based circuit authentication and applications." Massachusetts Institute of Technology, ACM Symposium on Applied Computing, 2003, Melbourne, FL.

line-of-sight for reading). Because RFID does not require line of sight, they may be deeply embedded or physically inaccessible, which can mean they are more difficult to swap out. Additionally, they may be read in groups of up to 100 rather than singly, saving time and allowing for some novel applications.[202]

RFID tags vary in functionality. The most common standard for RFID tags today is the Electronic Product Code (EPC) standard, which includes passive tags (without a self-contained power source) and active tags (power source included), which may further be read-only, write-once, or read-write capable.[203] Read-only or write-once tags are not particularly applicable to securing the supply of IT hardware components in combination with the previous recommendations because they would provide only a single, unchangeable identifier. PUFs embedded in the hardware components would essentially perform an identical function, with significantly increased assurance that neither the component nor the identifier could be cloned. The cloning of RFID chips themselves is of considerable concern; the most basic versions are too simple to support robust cryptographic security. Integration of PUFs into RFID chips has been explored as a possible solution to this problem, and seems technologically plausible,[204] though the additional circuitry could potentially multiply the cost of these cheap devices.

---

[202] Siemens. What is EPC? Brochure. Nürnberg: Author, 2006. RFID systems SIMATIC RF. 19 Aug. 2008 <http://www.automation.siemens.com/download/internet/cache/3/1455039/pub/de/wp_rfid_epc_e.pdf>.
[203] Siemens.
[204] Devadas, Srinivas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications." PUFCO, Inc., 2008 IEEE International Conference on RFID, 16-17 Apr. 2008, Las Vegas, NV.

The EPC Class 1 Generation 2 (EPC GEN-2) standard includes passive tags which support multiple rewrites.[205] Multiple rewrite capability allows data to be added to the chip as it passes scanning equipment. In addition to use by many private enterprises, EPC GEN-2 has been adopted and mandated for DoD suppliers in general in an effort to optimize the supply chain.[206] Using RFID to secure the supply chain of IT components, and particularly ICs, would require use of a standard with features similar to EPC GEN-2, in particular the multiple rewrite functionality. This would allow for implementation of security steps beyond simple identification, such as tracking. For example, tag readers could be placed at strategic points of the supply chain for the components. At each of these points, the readers could add location and time data to the chip, allowing for a complete picture of the transit path of the individual component. Deviations from the expected shipping schedule could be identified and flagged as suspicious to facilitate further inquiry. Research also supports the association of several tags that are simultaneously scanned through a process called *yoking*;[207] this could allow linking hardware components to the personnel that completed manufacturing, quality control, and testing steps, increasing accountability.

Any solution hinging on the application of RFID, however, should take into careful consideration the substantial body of evidence concerning the lack of security in this

---

[205] Siemens. What is EPC? Brochure. Nürnberg: Author, 2006. RFID systems SIMATIC RF. 19 Aug. 2008 <http://www.automation.siemens.com/download/internet/cache/3/1455039/pub/de/wp_rfid_epc_e.pdf>.
[206] "Radio Frequency Identification." Office of the Deputy Under Secretary of Defense (Logistics & Material Readiness). 11 June 2008. 19 Aug. 2008 <http://www.acq.osd.mil/log/rfid/rfid_faq.htm>.
[207] Juels, Ari. ""Yoking-Proofs" for RFID Tags." RSA Laboratories, First International Workshop on Pervasive Computing and Communication Security, 2004, Bedford, MA. RSA Laboratories. 19 Aug. 2008 <http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/rfidyoke/rfidyoke.pdf>.

technology currently. Passports based on RFID have been hacked and cloned,[208] and hackers report that tools to collect sensitive information from RFID-based credit cards like Paypass are readily available online.[209] Even the EPC GEN-2 standard, which has been broadly accepted by both public and private institutions, has suffered under analysis; researchers determined that passwords for interacting with EPC GEN-2 tags could be recovered one quarter of the time by an attacker who observed two to four transactions.[210] The combination of the other technological techniques described may provide sufficient security for hardware components while RFID security is under review.

Implementation of Technological Solutions

In order to effectively employ the preceding technological methods to secure the supply of IT hardware components for critical systems and networks, solutions must be correctly and thoroughly implemented. In order to illustrate the end-to-end process, the supply chain model (discussed earlier, starting on page 36) is referenced. In particular, the implementation of these solutions will be tied back to each supply chain phase, including design, manufacture and assembly, acquisition and shipping, and installation and use.

---

[208] Boggan, Steve. "'Fakeproof' e-passport is cloned in minutes." Times Online. 6 Aug. 2008.19 Aug. 2008 <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>.
[209] "Paypass: Easy to Use, Easy to Hack." Prime 9 News. CBS. KCAL, Los Angeles. 19 June 2008. Truveo. 19 Aug. 2008 <http://www.truveo.com/paypass-easy-to-use-easy-to-hack/id/996252795>.
[210] Peris-Lopez, Pedro, Tieyan Li, Tong-Lee Lim, Julio C. Hernandez-Castro, and Juan M. Estevez-Tapiador. "Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard." Carlos III University of Madrid and Institute for Infocomm Research, A*STAR Singapore, The 4th Workshop on RFID Security (RFIDsec08), 9-11 July 2008, Budapest, Hungary. 19 Aug. 2008 <http://events.iaik.tugraz.at/rfidsec08/papers/publication/06%20-%20peris-lopez%20-%20vulnerability%20analysis%20-%20paper.pdf>.

To begin, it is imperative that implementation of a proactive solution is embedded into the design phase. The integration of PUFs into IC designs should be investigated at the earliest opportunity and implemented with a preference for domestic designers. These designs must then be executed by manufacturers. The preference for domestic designers of hardware components allows for maintenance of gold standard designs to use for side-channel verification after the manufacture and assembly phase. Once the side-channel verification method outlined beginning on page 81 has been completed and verified for a family of ICs, chip PUFs should be registered with a domestic database. The combination of side-channel verification and PUFs allows for a unique identifier in each chip that is both unclonable and tamper-evident; any replacement or tampering will cause the IC to be unable to return a valid PUF "fingerprint". Throughout manufacturing, assembly, acquisition and shipping, RFID with improved security might be a viable option to increase accountability for subversive suppliers. However, subversion and counterfeiting at this stage would be revealed through verification of the PUF fingerprint at the last phase, installation and use.

CONCLUSION

As the research indicates, the question of addressing the threat of placing foreign-manufactured hardware in critical U.S. systems is not a simple, one-solution problem. As more of the manufacturing process is being offshored to several different countries, it has become clear that the current policy of trusting certain suppliers cannot guarantee the validity and security of hardware purchased from an untrusted environment on a long term basis. The recommendations provided allow for short term solutions to begin correcting the issue immediately, as well as long term solutions that will help maintain security in the future. The application of both the technology and policy recommendations is vital as both types of recommendations are necessary to approaching all sides of this complex issue.

FURTHER RESEARCH

After addressing the project question, the project team has determined that some additional research on certain topics that fell outside the scope of the project should be addressed. The recommendations for further investigations include:

- The possibility of creating an entirely domestic IT hardware manufacturing base for critical networks
- An examination of the ideological differences between geek culture and the government
- Continued investigation and research into secure technologies for tracking and shipping
- The creation of a comprehensive methodology exploring security measures at all levels for software, firmware, and hardware
- Further examination of the effectiveness and potential for industrial implementation of PUFs
- A cost analysis of the various recommendations proposed earlier.

Maintaining and enhancing domestic design and manufacturing is desirable for hardware that will be placed in critical U.S. systems. Though subversion and counterfeiting can occur anywhere, maintaining a domestic base for the production of critical components should decrease those chances, as well as provide more opportunity to monitor their production. Furthermore, there are also advantages to domestic manufacturing, which include decreased transport costs and increased security through avoidance of foreign

civil unrest. Though this may be a timely and costly endeavor, a domestic manufacturing base review must be completed.

As previously discussed in the geek culture section (page 56) broad philosophical differences exist between those in geek culture and the government. However, their existence does not imply that they are necessarily forever incompatible. Though the examination of these differences falls outside the scope of this topic, they do need attention in order to address problems outlined in previous sections

Although research has indicated great potential for tracking and shipping technologies such as RFID, additional research is necessary before wide-scale implementation in order to assess and address security weaknesses evident in the technology.

Throughout the course of research conducted, it was suggested by several industry experts that looking at one aspect of a system is not and will not be enough. Software, firmware, and hardware assurance must be examined in combination in order to ensure the security of a network or system as a whole.

Although literature provides support for the effectiveness of PUFs in a controlled research setting, it is less certain that they could be deployed on an industrial-level scale necessary to secure the entire supply of ICs. This should be examined in further detail.

Though each recommendation is strongly supported, a cost analysis should be conducted to examine the possibility of enacting proposed recommendations. A full analysis of the costs of each of the recommended solutions was beyond the scope of this project.

However, such an analysis would be necessary before these recommendations could be implemented.

BIBLIOGRAPHY

"2007 Salary Survey: Staff and Entry-level Positions." Computerworld. 18 Aug. 2008 <http://www.computerworld.com/spring/salary-survey.htm?activeyear=2007&type=job_levelmeter=0&page=1>.

Adsera, Alicia and Carles Boix. "Trade, Democracy, and the Size of the Public Sector: The Political Underpinnings of Openness." International Organization 56 (2002) 229-262.

AeA, Advancing the Business of Technology. Losing the Competitive Advantage? 2005. 17 July 2008. <http://www.aeanet.org/publications/idjj_CompetitivenessMain0205.asp>.

Agrawal, Dakshi, Selçuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. "Trojan Detection using IC Fingerprinting." IBM T.J. Watson Research Center and Worcester Polytechnic Institute, 2007 IEEE Symposium on Security and Privacy (SP'07), 20-23 May 2007, Berkeley, CA, USA.

"Alice.org." What is Alice? 28 July 2008 <http://www.alice.org/index.php?page=what_is_alice/what_is_alice>.

"Alice: A Wonderland." Carnegie Mellon. 1 Aug. 2008 <http://www.cmu.edu/homepage/practical/2007/fall/alice-a-wonderland.shtml>.

"Asymtek Applications Chip Encapsulation." Asymtek. 2008. 12 Aug. 2008 <http://www.asymtek.com/applications/chip_encapsulation.htm>.

"Authority of the FAR." Federal Acquisition Regulation, n.d.

Banga, Mainak, and Michael S. Hsiao. "A Region Based Approach for the Identification of Hardware Trojans." Virginia Polytechnic Institute, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08), 9 June 2008, Anaheim, CA.

Barboza, David. "Intel to Build Advanced Chip-Making Plant in China." The New York Times. 27 Mar. 2007.1 Aug. 2008 <http://www.nytimes.com/2007/03/27/technology/27chip.html>.

"BarCamp Wiki." BarCamp. 20 Aug. 2008 <http://barcamp.org/>.

"Beyond Pedigree: The Role of Infrastructure in the Pharmaceutical Supply Chain." Verisign. 7 July 2005. 6 Aug. 2008 <http://www.verisign.com/static/031078.pdf>.

Boggan, Steve. "'Fakeproof' e-passport is cloned in minutes." Times Online. 6 Aug. 2008.19 Aug. 2008 <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>.

Chao, Howard and Lawrence Sussman. 2003. "Semiconductor Investment Heats Up in China: A Legal and Tax Guide." Report, O'Melveny & Myers LLP.

Cognard, Anne, Robert Bednar, Bill Roweton, Noreen Ward, Linda Wells, and Deanna Zweifel. Procedures for the Identification of High-Ability Learners. Nebraska Department of Education. Lincoln: State of Nebraska, 1997.

Colonel Harman, Larry D. "Creativity: The Sustainer's Field of Dreams." U.S. Army Logistics Management College. 19 Aug. 2008 <http://www.almc.army.mil/alog/issues/marapr03/ms864.htm>.

"Commodity Trade Statistics Database 2006." United Nations Statistics Division. 6 June 2008. <http://comtrade.un.org.>

Cooper, W.H. "Government Procurement and U.S. Trade Policy. Congressional Research Service Report for Congress. March 10, 1995.

"Corruption Index." Transparency International. 2006. 6 June 2008. <http:www.transparencyinternational.org>.

Council on Competitiveness. Competitiveness Index: Where America Stands. 2007. 17 July 2008. <http://www.compete.org/images/uploads/File/PDF%20Files/Competitiveness_Index_Where_America_Stands_March_2007.pdf>.

"Counterfeit and Substandard Medicines." Impact: International Medical Products Anti-Counterfeiting Taskforce. 2008. World Health Organization. 18 June 2008 <https://www.who.int/medicines/services/counterfeit/en/>.

"Creative Commons." Creative Commons. 19 Aug. 2008 <http://creativecommons.org/>.

"Data Profiles." World Bank. 4 June 2008. <http:ddp-ext.worldbank.org/ext/ddpreports/>.

Davies Precision Machining Inc. v. U.S., 35 Fed. Cl. 651, 1996.

Defense Microelectronic Activity. "Trusted IC Supplier Accreditation Program." July 2008. <http://www.dmea.osd.mil/docs/AccreditatedSuppliers.pdf>

Defense Science Board. Future Strategic Strike Skills. March 2006. 17 July 2008. <http://www.acq.osd.mil/dsb/reports/2006-03-Skills_Report.pdf>.

Defense Science Board. High Performance Microchip Supply. Feb 2005. 19 July 2008. <http://www.cra.org/govaffairs/images/DSB.Appendix.D.pdf>

Devadas, Srinivas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications." PUFCO, Inc., 2008 IEEE International Conference on RFID, 16-17 Apr. 2008, Las Vegas, NV.

Domestic Policy Council Office of Science and Technology Policy. American Competitive Initiative. Feb 2006. 15 Aug 2008. <http://www.whitehouse.gov/stateoftheunion/2006/aci/aci06-booklet.pdf>.

Donley, Michael B. "Letter to Airmen." 13 Feb. 2006. 19 Aug. 2008 <http://www.af.mil/library/viewpoints/secaf.asp?id=217>.

"Entertainment Technology Center." Carnegie Mellon. 15 Aug 2008. <http://www.etc.cmu.edu/index.html>.

Faber, Paul. "RFID Strategy -- Pharmaceutical E-Pedigrees and RFID." IndustryWeek. 16 Oct. 2007. 12 July 2008 <http://www.industryweek.com/readarticle.aspx?articleid=15180>.

Federal Acquisition Regulation, Part 25, Subpart 25.1, Section 25.101. (FAC 2005-13): 25.1-4 through 25.1-5.

Federal Acquisition Regulation, Part 25, Subpart 25.1, Section 25.104. (FAC 2005-13): 25.1-5.

Federal Acquisition Regulation, Part 25, Subpart 25.1, Section 25.104. (FAC 2005-13): 25.1-6.

Federal Cyber Service: Scholarship For Service Information For Students. Oct 2005. 11 Aug 2008. <https://www.sfs.opm.gov/StudentBrochureWeb.pdf>.

Federation of American Scientists, "Intelligence Resource Program" National Security Presidential Directives, George W. Bush Administration, August 12, 2008.

Feng, Yi. "Political Freedom, Political Instability, and Policy Uncertainty: A Study of Political Institutions and Private Investment in Developing Countries" International Studies Quarterly 45 (2001) 271-294.

"Firmware Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/firmware>.

Fitzpatrick, Diane L. "Simple Science Experiments: Young Children Can Do Easy, Fun Science Projects At Home." Suite101. 8 Oct. 2007. 1 Aug. 2008 <http://parent-child-activities.suite101.com/article.cfm/simple_science_experiments>.

"Freedom in the World." Freedom House. 2006. 6 June 2008. <http:www.freedomhouse.org>.

Freeman, Richard B. "Does Globalization of the Scientific/Engineering Workforce Threaten U.S. Economic Leadership?" NBER Working Paper No. 11457. June 2005.

Gassend, Blaise, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. "Delay-based circuit authentication and applications." Massachusetts Institute of Technology, ACM Symposium on Applied Computing, 2003, Melbourne, FL.

Gassend, Blaise, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. "Silicon Physical Random Functions." Massachusetts Institute of Technology, Conference on Computer and Communications Security 2002, 18-22 Nov. 2002, Washington, D.C. Proceedings of the 9th ACM conference on Computer and communications security. Washington, D.C.: ACM, 2002.

Ginarte, Juan and Walter G. Park. "Determinants of Patent Rights: A cross-national study." Research Policy 26 (1997): 283-301.

Goldstein, Donald J. et al. USG Integrated Circuit Supply Chain Threat Opportunity Study. Institute for Defense Analyses. Jan 2006.

Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 21, 2005.

Grasso, Valerie Bailey. "The Berry Amendment: Requiring Defense Procurement to Come From Domestic Sources." CRS Report for Congress. April 30, 2008.

Grimes, J.G. "Clinger-Cohen Act (CCA), US Title 40, Knowledge Fair III, NDU/IRMC," Assistant Secretary Defense for Networks and Information Integration, June 27, 2006. <https://acc.dau.mil/GetAttachment.aspx?id=104272&pname=file&aid=23572>

"Hardware Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/hardware>.

"History." Creative Commons. 13 July 2007. 19 Aug. 2008 <http://wiki.creativecommons.org/history>.

Howell, Thomas R., et al. 2003. China's Emerging Semiconductor Industry. Semiconductor Industry Association and Dewey Ballantine LLP.

H.R. 2138 and S. 2209. 2006-2008. 05 Aug 2008. <washingtonwatch.com>.2006-2008. 05 Aug 2008. <washingtonwatch.com>.

"Index of Economic Freedom." Heritage Foundation. 2004-2006. 19 June 2008. <http://www.heritage.org/index/>.

"Industry Week Top 1000." Industry Week. 4 June 2008. <http:www.industryweek.com/research/iw1000/2007/iw1000rank.asp>.

Information Assurance Scholarship Program. 11 Aug 2008. <http://www.defenselink.mil/cio-nii/iasp/>.

"Information Assurance Specialist." USA Jobs. 07 Dec. 2007. 07 Aug. 2008 <http://jobsearch.usajobs.gov/getjob.asp?jobid=66135396&brd=3876&avsdm=2008%2d06%2d26+21%3a56%3a34&sort=rv&vw=d&q=%22information+assurance%22&logo=0&ss=0&customapplicant=15513%2c15514%2c15515%2c15669%2c15523%2c15512%2c15516%2c45575&tabnum=1&rc=5>.

Intel Corporation. "Fun facts: Exactly how small (and powerful) is 45 nanometers?" Fact sheet. Nov. 2007. 12 Aug. 2008 <http://www.intel.com/pressroom/kits/45nm/intel45nmfunfacts_final.pdf>.

Jin, Yier, and Yiorgos Makris. "Hardware Trojan Detection Using Path Delay Fingerprint." Yale University, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST '08), 9 June 2008, Anaheim, CA.

Jischke, Martin C. "Science Education in United States Reaches a Crossroads." Purdue University News. 24 Jan. 2006. Purdue University. 8 July 2008 <http://www.purdue.edu/UNS/html3month/2006/060124.SP-JIschke.rotary.html>.

Juels, Ari. ""Yoking-Proofs" for RFID Tags." RSA Laboratories, First International Workshop on Pervasive Computing and Communication Security, 2004, Bedford, MA. RSA Laboratories. 19 Aug. 2008 <http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/rfidyoke/rfidyoke.pdf>.

King, Samuel T, et al. "Designing and Implementing Malicious Hardware." University of Illinois (2006).

Knapp, L. A. "The Buy American Act: A Review and Assessment." Columbia Law Review, Vol. 61, No. 3, March 1961.

Koh, R., Edmund W. Schuster, Indy Chackrabarti, Attilio Bellman. 2003. White Paper: "Securing the Pharmaceutical Supply Chain." Massachusetts Institute of Technology, Auto-ID Center, June 1, 2003.

Konzack, Lars. "Geek Culture: The 3rd Counter-Culture." FNG2006. Preston, England. 15 July 2008.

Laychus, J., May, B. and Sadauskas, L. "Clinger-Cohen Act Implications for the Business Manager." United States Department of Defense, Deputy CIO PowerPoint, 2001.

Lee, Hau L. Supply Chain Security - Are You Ready? Stanford Global Supply Chain Management Forum. Sept 2004. 14 Aug 2008. <http://www.stanford.edu/group/scforum/Welcome/White%20Papers/SC_Security.pdf>.

Li, Quan and Adam Resnick. "Reversal of Fortune: Democratic Institutions and Foreign Direct Investment Inflows to Developing Countries." International Organization 57 (2003) 175-211.

Mann, Catherine L. and Jacob Funk Kirkegaard. Accelerating the Globalization of America The Role for Information Technology. Washington, D.C.: Institute for International Economics, 2006.

Markoff, John. "F.B.I. Says the Military Had Bogus Computer Gear." The New York Times. 9 May 2008. 17 June 2008.

Mayer, Marissa. "9 Notions of Innovation." Stanford University, Palo Alto, CA. 19 Aug. 2008.

McCormack, Richard. "Manufacturing & Technology News." 3 February 2004. Volume 11, No.3. June 2008. <http://www.manufacturingnews.com/news/04/0203/art1.html>

McGee, Marianne K. "Bill Gates Says Immigration, Education Reform Needed For U.S. To Compete." Information Week. 12 Mar. 2008. 18 July 2008 <http://www.informationweek.com/news/management/showarticle.jhtml?articleid=206903144>.

McGowan, A.S. and Vendryzk, V.P. "The Relation Between Cost Shifting and Segment Profitability in the Defense-Contracting Industry." The Accounting Review, Vol. 77, No. 4, October 2002, pp. 949-969.

McKinsey & Company. Addressing China's Looming Talent Shortage. Oct 2005. 19 July 2008. <http://www.mckinsey.com/mgi/reports/pdfs/China_talent/ChinaPerspective.pdf>.

"Measuring Globalization." Foreign Policy May/June 2005. 52-60.

Microsystems Technology Office. "Trust in Integrated Circuits (TIC)." 7 March 2007. <http://www.darpa.mil>

National Science Board. Science and Engineering Indicators. Two volumes. Arlington, VA: National Science Foundation (volume 1, NSB 08-01; volume 2, NSB 08-01A).

National Science Foundation. Federal Cyber Service: Scholarship For Service. 11 Aug 2008. <http://www.nsf.gov/pubs/2008/nsf08522/nsf08522.htm>.

National Security Agency. "Trusted Access Program Office (TAPO)." May 2008. <http://www.nsa.gov>

National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 are classified documents, but are referred to frequently in open-source literature as the current administration's executive "cyber initiative."

Navaretti, Giorgio Barb and Anthony J. Venables. Multinational Firms in the World Economy. Princeton, NJ: Princeton University Press, 2004.

"News Release: January 17, 2008: FERC approves new reliability standards for cyber security." United States Department of Energy, Federal Energy Regulatory Commission. <http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.pdf>

"No Child Left Behind." Ed.Gov. US Department of Education. 2 July 2008 <http://www.ed.gov/nclb/landing.jhtml?src=pb>.

Noorzoy, M.S. "'Buy American' as an Instrument of Policy." The Canadian Journal of Economics, Vol. 1, No. 1, February 1968.

Nye, Joseph S. "The Decline of America's Soft Power." Foreign Affairs. May-June 2004. The Council of Foreign Relations. 25 Aug. 2008 <http://www.foreignaffairs.org/20040501facomment83303/joseph-s-nye-jr/the-decline-of-america-s-soft-power.html>.

"Origin of the Term "Black Box"" Google Answers. 2002. 19 Aug. 2008 <http://answers.google.com/answers/threadview?id=114741>.

Parker, Ron. Foreign IT Roundtable, Washington, D.C. 4 June 2008. Interview conducted by the authors.

"Paypass: Easy to Use, Easy to Hack." Prime 9 News. CBS. KCAL, Los Angeles. 19 June 2008. Truveo. 19 Aug. 2008 <http://www.truveo.com/paypass-easy-to-use-easy-to-hack/id/996252795>.

Peris-Lopez, Pedro, Tieyan Li, Tong-Lee Lim, Julio C. Hernandez-Castro, and Juan M. Estevez-Tapiador. "Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard." Carlos III University of Madrid and Institute for Infocomm Research, A*STAR Singapore, The 4th Workshop on RFID Security (RFIDsec08), 9-11 July 2008, Budapest, Hungary. 19 Aug. 2008 <http://events.iaik.tugraz.at/rfidsec08/papers/publication/06%20-%20peris-lopez%20-%20vulnerability%20analysis%20-%20paper.pdf>.

Personal interview with Department of Homeland Security officials. 10 July 2008.

Personal interview with Information Assurance expert. 29 May 2008.

Pope, Sydney. "Trusted Integrated Circuit Strategy." IEEE Transactions on Components and Packaging Technologies 31:1 (2008) 230-234.

Poynder, Richard. "The Open Source Movement." Information Today. Oct. 2001. 19 Aug. 2008 <http://www.infotoday.com/it/oct01/poynder.htm>.

"Pre-Employment Programme." ExxonMobil. 15 Aug 2008. <http://www.exxonmobil.com.sg/AP-English/Jobs/SG_Work_preemployment.asp>.

"Preschool Science Fun and Experiments." Child Care Lounge. 1 Aug. 2008 <http://www.childcarelounge.com/caregivers/sciencefun.htm>.

"Product counterfeiting." Global Legal Information Network. Library of Congress. 31 July 2008 <http://www.glin.gov/subjecttermindex.action>.

"Radio Frequency Identification." Office of the Deputy Under Secretary of Defense (Logistics & Material Readiness). 11 June 2008. 19 Aug. 2008 <http://www.acq.osd.mil/log/rfid/rfid_faq.htm>.

"Regulatory Procedures Manual March 2008 Chapter 9 Import Procedures." ORA Import Program. Mar. 2008. US Food and Drug Administration. 24 June 2008 <http://www.fda.gov/ora/import/ora_import_program.html>.

Roldan, Raul. "FBI Criminal Investigation: Cisco Routers." Power Point Presentation (2008).

RSS Advisory Board. "RSS 2.0 Specification." RSS Advisory Board. 18 Aug. 2008 <http://www.rssboard.org/rss-specification>.

Rumsfeld, Donald H. "U.S. Joint Forces Command Change-of-Command Ceremony." U.S. Joint Forces Command Change-of-Command Ceremony. Norfolk, VA. Defense Link. 02 Oct. 2008. 19 Aug. 2008 <http://www.defenselink.mil/speeches/speech.aspx?speechid=294>.

Rybicki, Jim. Departments of Justice and Homeland Security Announce International Initiative Against Traffickers In Counterfeit Network Hardware (Press Release). Federal Bureau of Investigation. Washington Field Division. 2008.

Scalise, George. "China's High-Technology Development." Testimony before the US China Economic and Security Review Commission. April 21, 2005.

Seifert, J.W. "Information Technology (IT) Management: The Clinger-Cohen Act and the Homeland Security Act of 2002." CRS Report for Congress. February 3, 2005.

Semiconductor Manufacturing International Corporation. "SMIC and IBM Sign Licensing Agreement." Press release. 26 Dec. 2007. 12 Aug. 2008 <http://www.prnewswire.com/cgi-bin/stories.pl?acct=104&story=/www/story/12-26-2007/0004727846&edate=>.

Siemens. What is EPC? Brochure. Nürnberg: Author, 2006. RFID systems SIMATIC RF. 19 Aug. 2008 <http://www.automation.siemens.com/download/internet/cache/3/1455039/pub/de/wp_rfid_epc_e.pdf>.

"Software Definition." TechTerms. 5 Dec. 2006. 14 July 2008 <http://www.techterms.com/definition/software>.

"Special 301 Report." Office of the United States Trade Representative. 30 May 2008. <http:www.ustr.gov>.

"Statistical Program." Network of World Merchandise Trade. 11 June 2008. <http:www.stat.wto.org/StatisticalProgram/WSDBViewData.aspx?Language=E>.

"TAPO Welcome Page." TAPO: Trusted Access Program Office. 2 July 2008 <https://www.tapoffice.org/tapo.html>.

Tatelman, Todd B. "International Government-Procurement Obligations of the United States: An Overview." CRS Report for Congress, May 17, 2005.

Tech Talk. "Trust in Integrated Circuits." June 2008. <http://blogs.spectrum.iee.org/tech_talk/2008/05/trust_in_integrated_circuits.html>

"The China Price." BusinessWeek. Dec 2004. 19 July 2008. <http://www.businessweek.com/magazine/content/04_49/b3911401.htm>.

The Library of Congress, Bills and Resolutions. 07 Aug 2008. <http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.5630>.

The President's Council of Advisors on Science and Technology. Sustaining the Nation's Innovation Ecosystems. Jan 2004. 17 July 2008. <http://www.ostp.gov/pdf/finalpcastsecapabilitiespackage.pdf>.

The Programme for International Student Assessment (PISA). Organisation for Economic Co-operation and Development. 2006.

"The Semiconductor Integrated Circuits Layout Designs - IPR Toolkit." US Embassy New Delhi, India. U.S. State Department. 11 Aug. 2008 <http://newdelhi.usembassy.gov/iprsemicond.html>.

"The Seven Army Values." 10 Oct. 2003. 19 Aug. 2008 <http://www.history.army.mil/lc/the%20mission/the_seven_army_values.htm>.

"Too Much Testing?" CBS News. 4 Apr. 2006. 18 July 2008 <http://www.cbsnews.com/stories/2006/04/04/eveningnews/main1472010.shtml>.

"Trade Agreement Act of 1979." United States of America Department of State: International Information Programs, n.d.

United States Code. Title 40, Subtitle III, Chapter 113. Cornell University Law School.

United States Code: Title 10, Subpart A, Part I, Chapter 7. Cornell University Law School.

United States Code: Title 40, Subtitle III, Chapter 111, §11103, subsection (b). Cornell University Law School.

United States Code: Title 41, Chapter 7. Cornell University Law School. <http://www4.law.cornell.edu/uscode/html/uscode41/usc_sup_01_41_10_7.html>

United States Department of Defense. "About Defense Acquisition Regulations System." Defense Procurement, Acquisition Policy, and Strategic Sourcing." <http://www.acq.osd.mil/dpap/dars/about.html>

United States Department of Defense. "Clinger-Cohen Act and Related Documents." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>

United States Department of Defense. "Clinger-Cohen Act and Related Documents: Foreword." July 2008. <http://www.army.mil/armybtkc/docs/CCA-Book-Final.pdf>

United States Department of Defense. "Improving Information Technology (IT) Investment Management and Oversight: From Clinger Cohen Act (CCA) to DoD Transformation." Executive Briefing and Project Report, Deputy CIO, Commercial Policies and Oversight, Acquisition, Technology and Logistics, March 3, 2005.

United States Department of Defense. Defense Procurement, Acquisition Policy, and Strategic Sourcing. <http://www.acq.osd.mil/dpap/index.html>

United States Government Accountability Office. Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India. Sept 2006. 14 Aug 2008. <http://www.gao.gov/new.items/d06423.pdf>.

United States. Department of Defense. Department of Defense Dictionary of Military and Related Terms (JP 1-02). 30 May 2008. 14 July 2008 <http://www.dtic.mil/doctrine/jel/doddict>.

United States. Department of Defense. Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics. Defense Science Task Force Board On High Performance Microchip Supply. Feb. 2005. 30 May 2008 <http://www.acq.osd.mil/dsb/reports/2005-02-hpms_report_final.pdf>.

United States. Government Accountability Office. 2006. Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by by Sectors' Characteristics. October 2006.

United States. Government Accountability Office. 2008. Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruptions on Converged Voice and Data Networks, page 2-3. June 2008.

United States. Government Accountability Office. Offshoring: U.S. Semiconductor and Software Industries Increasingly Produce in China and India. Sept 2006. 14 Aug 2008. <http://www.gao.gov/new.idems/d06423.pdf>

United States. National Mathematics Advisory Panel. Department of Education. The Final Report of the National Mathematics Advisory Panel. 2008.

University of Nebraska at Omaha. Aim for the Stars. 2005. 18 July 2008. http://www.unomaha.edu/aimforthestars/

University of Nebraska at Omaha. "Complete List of Camps." Aim for the Stars. 2005. 18 July 2008 <http://www.unomaha.edu/aimforthestars/pages/allcamps.php>.

Van den Berg, Hendrik. Economic Growth and Development. Boston, MA: McGraw Hill, 2001.

Vu, Pauline. "Do State Tests Make the Grade?" Stateline.Org. 17 Jan. 2008. 27 June 2008 <http://www.stateline.org/live/details/story?contentId=272382>.

Wack, John P., and Stanley A. Kurzban. NCSL Bulletin: Advising users on computer systems technology. National Institute of Standards and Technology. National Computer Systems Laboratory. 1990. National Institute of

Standards and Technology. Aug. 1990. 31 July 2008 <http://csrc.nist.gov/publications/nistbul/csl90-08.txt>.

"Wafer and Die Foundries and Distributors." Chip Directory. 12 June 2008. <http://www.xs4all.nl>.

Wang, Xiaoxiao, Mohammad Tehranipoor, and Jim Plusquellic. "Detecting Malicious Inclusions in Secure Hardware: Challenges and Solutions." University of Connecticut and University of New Mexico, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, 9 June 2008, Anaheim, CA.

Weiss, Gus W. "The Farewell Dossier." Duping the Soviets. (New York, 2005): 121-126.

Wilson, Clay. United States. Foreign Affairs, Defense, and Trade Division. Congressional Research Service. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 1 Apr. 2005. 24 July 2008 <http://usinfo.state.gov/infousa/government/overview/docs/RL32114.pdf>.

Wilson, Daniel. "The Rise and Spread of State R&D Tax Credits." FRBSF Economic Letter 2005-26. 07 Aug 2008. <http://www.frbsf.org/publications/economics/letter/2005/el2005-26.pdf>.

Winerip, Michael. "Standardized Tests Face a Crisis Over Standards." Education Sector. 22 Mar. 2006. 18 July 2008 <http://www.educationsector.org/media/media_show.htm?doc_id=362581>.

Wolff, Francis, Chris Papachristou, Swarup Bhunia, and Rajat S. Chakraborty. "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme." Case Western Reserve University, Cleveland, Ohio, USA, Design, Automation and Test in Europe, 2008 (DATE '08), 10-14 Mar. 2008, Munich, Germany. 1362-365.

"World Investment Report 2007." United Nations Conference on Trade and Development. (New York: United Nations, 2007).

"World Military Spending." Global Issues. 19 July 2008. <http://www.globalissues.org/Geopolitics/ArmsTrade/Spending.asp#WorldMilitarySpending>.

World Trade Organization. DISPUTE SETTLEMENT: DISPUTE DS309 China - Value-Added Tax on Integrated Circuits. 11 Aug 2008. <http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds309_e.htm>.

Zimmerman, B. "Acquisition of Information Technology." Defense Acquisition University, West Region, May 23, 2007.

APPENDIX A: INVESTMENT ENVIRONMENTS

As noted in the economic realities section (page 31), the global economic trend is moving towards a greater degree of globalization and interdependence; this is also true of the IT industry. Approximately 170 MNEs are engaged in IT hardware design or manufacturing of some kind, and these corporations utilize thousands of subcontractors.[211] These relationships cross borders with firms in over thirty countries engaged in a substantial amount of IC chip design and manufacturing activities.[212] When examining these relationships, it is apparent that the nation-states involved represent a widely diverse political and economic spectrum ranging from democracies to authoritarian regimes. Economic intervention in the various states varies widely as well.

The academic literature on FDI is extensive. Most scholars have focused on the role of FDI in specific bilateral relationships, such as between the United States and the United Kingdom. Others have focused on FDI and democracy, either looking at whether substantial investments in a state improve its adherence to international norms of democracy over time,[213] or examining the relationship between outgoing FDI and democracy, finding that consolidated democracies tend to make greater commitments to outgoing FDI.[214] Further studies have examined the relationship between stable

---

[211] "Industry Week Top 1000." Industry Week. 4 June 2008. <http:www.industryweek.com/research/iw1000/2007/iw1000rank.asp>.
[212] "Wafer and Die Foundries and Distributors." Chip Directory. 12 June 2008. <http://www.xs4all.nl>.
[213] Li, Quan and Adam Resnick. "Reversal of Fortune: Democratic Institutions and Foreign Direct Investment Inflows to Developing Countries." International Organization 57 (2003) 175-211.
[214] Li, Quan & Adam Resnick.

authoritarian regimes, unstable revolutionary environments, and FDI.[215] Such studies report mixed results; while data from earlier time periods seems to indicate that FDI inflows are directly related to enhanced democratic performance, others have suggested that many international corporations maintain working relationships with stable authoritarian regimes.[216] This factor of stability is important as no investor appears to be willing to risk profit margins or normal flow of trade by placing itself in a chaotic environment. However, stability offered by consolidated authoritarian regimes appears to attract investment.[217]

Though literature presents a mixed picture, it does seem to indicate that investors and MNEs value government stability, environments that do not present extensive rent prices, and the opportunity to take advantage of monopoly-like conditions. While the relative strength of FDI relationships appears to be greatest between democracies or between neighboring states, emerging relationships between authoritarian regimes and democracies are on the rise.[218] This situation sets the stage for an environment in which the sorts of phenomenon related to the topic of this paper may be possible.

In this section, a variety of economic and political factors will be examined with the goal of uncovering relationships related to the focus of this paper. The analysis provided

---

[215] Feng, Yi. "Political Freedom, Political Instability, and Policy Uncertainty: A Study of Political Institutions and Private Investment in Developing Countries" International Studies Quarterly 45 (2001) 271-294.
[216] Li, Quan and Adam Resnick. "Reversal of Fortune: Democratic Institutions and Foreign Direct Investment Inflows to Developing Countries." International Organization 57 (2003) 175-211.
[217] Adsera, Alicia and Carles Boix. "Trade, Democracy, and the Size of the Public Sector: The Political Underpinnings of Openness." International Organization 56 (2002) 229-262.
[218] "World Investment Report 2007." United Nations Conference on Trade and Development. (New York: United Nations, 2007).

below examines such factors within nation-states to determine if they produce an environment that is conducive to counterfeiting and subversion activities.

A wide range of journalistic reporting indicates that certain states may be engaged in such activities. Various government "watch lists" also exist that highlight intellectual property rights (IPR) violations in various states.[219] However, there is a dramatic difference between qualitative or journalistic reporting and empirical evidence. There is no categorical listing of prosecutions of IPR violations, or even complaints. Certainly legal cases have been filed regarding IPR violations;[220] however, parsing through documents for specific cases would not only be beyond the capabilities of this time-limited project, it would perhaps also fail to represent the true number of counterfeiting operations, with subversion being even more difficult to empirically capture at an unclassified level.

Therefore, a more general model was created to examine whether environments in which counterfeiting or subversion is more likely can possibility be determined through open-source data. This section will introduce a number of independent and dependent variables and will analyze their relationships with the hope of uncovering correlations. Clearly, relationships that are found are tentative. Such a framework may prove exceptionally valuable, especially if classified or more extensive data could be used. A variety of factors suggest themselves as potential causal factors, as listed below:

- GDP Growth

[219] "Special 301 Report." Office of the United States Trade Representative. 30 May 2008. <http:www.ustr.gov>
[220] "Special 301 Report."

- GDP Per Capita (PPP)
- Population
- Work force engaged in technical and manufacturing jobs
- A Conflict Variable
- Military Spending as a percentage of GDP
- Percentage of High Technology Exports
- Percentage of World High Technology Market Captured by the State
- Incoming FDI (Foreign Direct Investment) Levels

It is likely that some environments present a higher risk of counterfeiting and subversion. Although authoritative classification of these environments is unlikely, a number of indices serve as potential indicators. As indices are generally assumed to contain some element of subjectivity, several have been selected to provide a variety of test cases. These include the Freedom House Political Rights and Civil Liberties,[221] the Transparency International Corruption Rankings,[222] the Heritage Foundation's Property Rights and Government Size Index,[223] and the Ginarte and Park Intellectual Property Rights Patent Index.[224]

---

[221] "Freedom in the World." Freedom House. 2006. 6 June 2008. <http:www.freedomhouse.org>
[222] "Corruption Index." Transparency International. 6 June 2006. <http:www.transparencyinternational.org>
[223] "Index of Economic Freedom." Heritage Foundation. 2005-2008. 19 June 2008. <http://www.hertiage.org/index>
[224] Ginarte, Juan and Walter G. Park. "Determinants of Patent Rights: A cross-national study." Research Policy 26 (1997): 283-301.

A dummy variable is also presented representing the presence (or absence) of a particular state on the U.S. Trade Representative's IP "Watch List".[225] Rankings from these indices for the year 2006 are consolidated into the following table.

State	Corrupt Index	PR Score	CL Score	H Prop Rights	H Gov't Size	Park IP Index	Watch List	Summary
Belgium	7.1	1	1	90	26.79	4.67	No	0 of 7
Brazil	3.5	2	2	50	71.73	3.59	Yes	3 of 7
Canada	8.7	1	1	90	53.43	4.67	Yes	1 of 7
China	3.5	7	6	30	86	3.08	Yes	7 of 7
Croatia	4.1	2	2	30	23.19	.	No	2 of 7
Czech Republic	5.2	1	1	70	36.8	4.33	Yes	3 of 7
Finland	9.4	1	1	90	24.4	4.67	No	0 of 7
France	7.2	1	1	70	11.22	4.67	No	1 of 7
Germany	7.8	1	1	90	31.74	4.5	No	0 of 7
Hungary	5.3	1	1	70	27.09	4.5	Yes	3 of 7
Ireland	7.5	1	1	90	64.71	4.67	No	0 of 7
Italy	5.2	1	1	50	29.14	4.67	Yes	3 of 7
Japan	7.5	1	2	70	58.26	4.67	No	1 of 7
Malaysia	5	4	4	50	75.2	3.48	Yes	7 of 7
Mexico	3.5	2	2	50	82.14	3.88	Yes	4 of 7
Netherlands	9	1	1	90	29.14	4.67	No	0 of 7
Poland	4.2	1	1	50	39.52	4.21	Yes	3 of 7
Singapore	9.3	5	4	90	89.62	4.21	No	4 of 7
Slovakia	4.9	1	1	50	52.48	4.21	No	2 of 7
South Korea	5.1	1	2	70	77.64	4.33	No	3 of 7
Sweden	9.3	1	1	90	3	4.54	No	0 of 7
Switzerland	9	1	1	90	61.12	4.33	No	0 of 7
Taiwan	5.7	1	1	70	83.99	3.74	Yes	5 of 7
Turkey	4.1	3	3	50	68.12	4.01	No	4 of 7
UK	8.5	1	1	90	43.9	4.54	No	0 of 7
USA	7.2	1	1	90	61.12	4.88	No	0 of 7

Table 5: Consolidated Rankings, 2006

These variables each use a different methodology and coding system. For instance, Freedom House uses surveys of citizens in private life, government, and of visitors to produce its rankings. A "1" represents the highest levels of freedom, while "7" represents the least. Transparency International measures perceived levels of corruption within

[225] "Special 301 Report." Office of the United States Trade Representative. 30 May 2008. <http:www.ustr.gov>

business and government. Transparency International also uses surveys to gather data, but presents a reversed scoring system. In this system, a "1" represents the greatest levels of corruption, while a "10" represents the lowest levels of corruption.[226]

The Heritage Foundation Index of Economic Freedoms contains two measures of interest to this study: Property rights and government size. Property rights measures the viability of contracts, levels of adherence to international IP agreements, and the independence and power of the judiciary when considering property rights. A score of "0" represents the worst possible environment, while a score of "100" indicates the best. Government size represents the size of public sector spending, the levels of government ownership of business. In this ranking system, the methodology is reversed, with low scores indicating greater levels of government intrusiveness.[227]

The Ginarte and Park Intellectual Property Rights Index considers a variety of data and is one of the first academic indexes to focus specifically on patent and intellectual property rights. In this index, a "5" represents the highest levels of adherence to these principles, while a "0" represents the least.[228]

Finally, the United States Trade Representative (USTR) publishes an IP "Watch List" for business and government leaders that indicate the presence of IP violations within particular states. As this report is not based on empirical measures, it is coded as a simple

---

[226] "Freedom in the World." Freedom House. 2006. 6 June 2008. <http:www.freedomhouse.org>
[227] "Index of Economic Freedom." Heritage Foundation. 2005-2008. 19 June 2008. <http://www.hertiage.org/index>
[228] Ginarte, Juan and Walter G. Park. "Determinants of Patent Rights: A cross-national study." Research Policy 26 (1997): 283-301.

dummy variable, with "0" indicating that a state is not on the list, and "1" indicating that a state is on the watch list.[229]

A regression analysis using these variables will be presented. This analysis will test the most promising correlative relationships. Adjusted r^2 scores, overall model significance, and standardized coefficients, and individual variable significance will be presented. Additionally, variance inflation factor (VIF) scores will be reported for each variable to reveal the possibility of multicollinearity, or multiple variables combining to produce an effect.

A collection of data from all states that currently engage in significant levels of IT hardware production is presented. 78 cases representing 26 nation-states during the time span of 2004, 2005, and 2006 are provided; a list of these nation-states is presented below in alphabetical order.

Belgium	France	Mexico	Switzerland
Brazil	Germany	Netherlands	Taiwan
Canada	Hungary	Poland	Turkey
China	Ireland	Republic of Korea	United Kingdom
Croatia	Italy	Singapore	United States
Czech Republic	Japan	Slovakia	
Finland	Malaysia	Sweden	

Table 6: Major IC Exporting States[230]

In those cases when data was not available for a particular state or year, it was coded as "missing". It should be noted that there were few missing cases in this data base.

[229] "Index of Economic Freedom." Heritage Foundation. 2005-2008. 19 June 2008. <http://www.hertiage.org/index>
[230] "World Investment Report 2007." United Nations Conference on Trade and Development. (New York: United Nations, 2007).

Some may question the selection of these particular nation-states for the analysis. Research indicates that these nation-states represent the top semi-conductor producers in the world. There are several nations, such as Russia and India, that are heavily engaged in the IT software field that are not as invested in hardware design, development, and manufacturing.[231] However, these activities may migrate to such countries when capabilities match wage and product costs, or at a point when these states provide attractive tax or other financial incentives for outsourcing opportunities in IT hardware production.

The data indicates the dominance of several key states within the semiconductor field. These figures also represent states that import IC chips for assembly and resale. The top state importers and exporters of semiconductors are listed below:

State	Revenue (in mil $)	Percentage
China	579	33.3%
Singapore	423	24.3%
United States	231	13.3%
Germany	70	4.0%
United Kingdom	61	3.5%
Others	374	21.5%
Total	1,740	

Table 7: Top State Importers of Semiconductors[232]

[231] "Data Profiles." World Bank. 4 June 2008. <http:ddp-ext.worldbank.org/ext/ddpreports/>.
[232] "Commodity Trade Statistics Database 2006." United Nations Statistics Division. 6 June 2008. <http://comtrade.un.org.>

State	Revenue (in mil $)	Percentage
United States	1538	50.9%
Singapore	720	23.8%
China	334	11.1%
Germany	136	4.5%
United Kingdom	48	1.6%
Others	240	7.9%
Total	3,019	

Table 8: Top State Exporters of Semiconductors[233]

These figures do not indicate how much a particular state's corporations outsource chip design and fabrication to states with more advantageous economic climates. However, research indicates that it is prevalent, especially from states with high GDP per capita to states with low GDP per capita.[234]

GDP growth is a term that expresses the growth rate of Gross Domestic Product, or the value of goods produced within a nation state as a percentage. A figure over 2% is thought to suggest a quickly expanding economy. Rates under 2% indicate a stagnant or recessionary economy. For the purposes of this paper, it is hypothesized that a state seeking and obtaining large amounts of FDI and participating in incoming outsourcing agreements would tend to have a higher growth rate. This measure is expressed in Purchasing Power Parity (PPP) terms, a calculation that allows these figures to be compared between states by balancing these them with the relative value of each state's currency on the currency market.

---

[233] "Commodity Trade Statistics Database 2006." United Nations Statistics Division. 6 June 2008. <http://comtrade.un.org.>

[234] "World Investment Report 2007." United Nations Conference on Trade and Development. (New York: United Nations, 2007).

GDP Per Capita (PPP) is another commonly used indicator that divides total GDP by population, roughly displaying the "average income" of each person within a state. For this research, states with low GDP Per Capita (PPP) could be attractive places for outsourcing, as their labor costs would be relatively lower. Of course, figures that are exceptionally low could also be indicative of a lack of suitable labor and infrastructure requirements.

The population variable used in this study provides the number of citizens within a state. It may be that higher population levels may prevent the state from efficiently managing and controlling corruption, and, by proxy, counterfeiting operations. Alternatively, a large population also represents a larger market for consumer products, an important consideration for corporate investment.

One might suggest that if a corporation wished to offshore a high tech manufacturing facility, they would want to ensure that workers in the chosen state are capable of the work. As such, a measure of work force engaged in technical and manufacturing jobs is presented as a variable.

Internal stability, or the lack of military conflict in an environment, would also seem to be important to firms making investment decisions within a state. Constant war or internal conflict would seem to create a poor investment environment. Thus a variable based on the Correlates of War project conflict variable is also tested.

Military spending as a percentage of GDP indicates levels of military spending within a state. These figures may be reported differently depending on the structure of the state.

High levels of military spending may be attractive to foreign investors due to presumed increase in stability, or unattractive due to perceived authoritarianism.

The percentage of high technology exports refers to the amount of IT and technologically advanced exports the state produces. Because states displaying higher levels of these exports produce or assemble the IT hardware the US relies on, it may present them with a greater opportunity to counterfeit or subvert critical U.S. hardware, if desired.

The percentage of the world market captured indicates the market penetration in high technology products by industries of the state. A high level is indicative of extensive amounts of the state's industries' products on the market.

Incoming and outgoing FDI levels indicate the amount of foreign investment either entering the state or investments made by the state in other countries. A high level of incoming FDI is indicative of high level of outsourcing to, or investment in, the state's firms.[235] Outgoing FDI points to the relative power of the state's economy.[236]

---

[235] "World Investment Report 2007." United Nations Conference on Trade and Development. (New York: United Nations, 2007).
[236] "Measuring Globalization." Foreign Policy May/June 2005. 52-60.

State	Incoming FDI	Outgoing FDI
Belgium	$ 71,997,000,000	$ 63,005,000,000
Brazil	$ 18,782,000,000	$ 28,202,000,000
Canada	$ 27,000,000,000	$ 45,243,000,000
China	$ 69,468,000,000	$ 16,130,000,000
Croatia	$ 3,556,000,000	$ 212,000,000
Czech Republic	$ 5,957,000,000	$ 1,556,000,000
Finland	$ 3,706,000,000	$ 9,000,000
France	$ 81,076,000,000	$ 115,036,000,000
Germany	$ 42,870,000,000	$ 79,427,000,000
Hungary	$ 6,098,000,000	$ 3,016,000,000
Ireland	$ (12,811,000,000)	$ 22,101,000,000
Italy	$ 39,159,000,000	$ 42,035,000,000
Japan	$ (6,506,000,000)	$ 50,266,000,000
Korea, Republic	$ 4,950,000,000	$ 7,129,000,000
Malaysia	$ 6,090,000,000	$ 6,005,000,000
Mexico	$ 19,037,000,000	$ 5,758,000,000
Netherlands	$ 4,371,000,000	$ 22,692,000,000
Poland	$ 13,922,000,000	$ 4,266,000,000
Singapore	$ 24,207,000,000	$ 8,626,000,000
Slovakia	$ 4,165,000,000	$ 368,000,000
Sweden	$ 27,231,000,000	$ 24,600,000,000
Switzerland	$ 25,089,000,000	$ 81,505,000,000
Taiwan	$ 7,424,000,000	$ 7,399,000,000
Turkey	$ 20,120,000,000	$ 934,000,000
United Kingdom	$ 139,000,000,000	$ 79,000,000,000
USA	$ 175,394,000,000	$ 216,614,000,000

Table 9: Incoming and Outgoing FDI of IT Exporting Countries[237]

It may be suggested that such relationships could lead the recipient of FDI to overlook IPR violations, or allow agents of the investing state's firms to control otherwise impenetrable industrial processes, potentially laying the groundwork for state-sponsored subversion activities.

[237] "Commodity Trade Statistics Database 2006." United Nations Statistics Division. 6 June 2008. <http://comtrade.un.org.>

A series of six models was created testing the variables discussed above. Each model removes a particular dichotomous index variable and replaces it with another index to reveal improving relationships. This process allows for a robust test of all variables concerned. The P score, adjusted r^2 scores, variable significance, and VIF statistic are reported for all variables.

Ind. Variables	Mod 1	VIF	Mod 2	VIF	Mod 3	VIF	Mod 4	VIF	Mod 5	VIF	Mod 6	VIF
GDP Growth	.443	1.623	.304	1.505	.512	1.504	.306	1.487	.368	1.496	.341	1.48
GDP Per Capita	.079	5.142	.004	4.837	.220	3.154	.685	3.714	.050	5.212	.003	2.197
Military Spending	.006	1.328	.009	1.369	.001	1.359	.000	1.393	.005	1.329	.004	1.34
Tech Exports	.365	1.473	.633	1.671	.267	2.502	.197	2.218	.315	1.501	.881	1.996
Park IP Index	.817	3.187	-	-	-	-	-	-	-	-	-	-
Watch List	.838	2.143	.607	2.007	.600	1.780	.662	1.760	.894	1.748	.823	1.923
Work Force	.010	1.976	.048	2.361	.000	2.417	.000	2.309	.015	2.350	.005	1.965
Conflict	.267	3.024	.115	3.227	.026	3.190	.014	3.155	.225	2.917	.172	2.811
Corruption Index	-	-	.282	5.140	-	-	-	-	-	-	-	-
PR Score	-	-	-	-	.006	5.410	-	-	-	-	-	-
CL Score	-	-	-	-	-	-	.001	5.420	-	-	-	-
Property Rights	-	-	-	-	-	-	-	-	.912	4.354	-	-
Government Size	-	-	-	-	-	-	-	-	-	-	.195	2.046
Adjusted r^2	**0.353**		**0.375**		**0.432**		**0.462**		**0.364**		**0.381**	
P	**.000**		**.000**		**.000**		**.000**		**.000**		**.000**	

Table 10: Models and Results

Model one reports a robust P score of .000, and an adjusted r^2 score of .353. The military spending and work force variables are the only two significant variables. Both variables are significant at the .01 level. Notably, the Park IP index, a measure of adherence to patent laws, is not statistically significant.

Model two substitutes Transparency International's Corruption Index for the Park Index. This model also displays robust P and adjusted r^2 scores. GDP Per capita becomes

statistically significant at the .005 level, but displays a troubling VIF statistic of 4.837. Thus, this variable should be considered insignificant. However, the military spending and work force variables remain significant at the .01 level. The corruption index is not statistically significant.

Model three retains a robust P score of .000 and adjusted r^2 score of .432. This model substitutes the Freedom House Political Rights index for the Corruption Index. The Political Rights variable presents a statistically significant result at the .01 level. However, it also presents a problematic VIF statistic of 5.410. Military spending (.001) and work force (.000) remain highly significant variables. The conflict variable becomes statistically significant for the first time at the .05 level.

Model four remains strongly significant with a P score of .000 and presents the highest adjusted r^2 score of all the models tested at .462. The military spending and work force variables remain significant at the .000 level, while the conflict variable also presents a significant relationship at the .05 level. The Freedom House civil liberties score also presents a significant result, but is again problematic with a VIF score of 5.420.

Model five remains robust with a P score of .000 and an adjusted r^2 score of .364. This model substitutes the Heritage Foundation's Property Rights index, a measure of access to effective courts, property rights protection, and intellectual property rights importance. In addition to the military spending (.005) and the work force (.05) variables, GDP per capita presents a statistically significant result (.05). However, GDP per capita also presents a worrying VIF statistic of 5.212.

Finally, Model 6 remains highly significant with a P score of .000 and an adjusted r^2 score of .381. This model substitutes the Heritage Foundations' government size index, a combined measure of government intrusion into business decisions and levels of public sector spending. GDP per capita (.005), military spending (.005) and work force (.005) present highly significant results with solid VIF statistics. The government variable is not statistically significant.

Across all six models, the work force and military spending variables are the only variables to remain significant. The conflict variable is significant in two of the six models tested. GDP per capita is significant in three of the six models, but two of these findings are invalidated by poor VIF results.

To summarize, the results presented by the four models indicate that the size of a state's suitable work force and its levels of military spending are the primary influences on incoming FDI. These variables also presented high standardized beta scores. None of the indices of corruption, political freedoms, or institutionalized government intrusion into business markets were consistently significant in the models analyzed.

As a follow-up, China was removed from the model to provide a control for the presence of statistically outlying states with extreme scores in one direction or another. The control test of the model removing China retained the same relationships as the models tested, although it weakened the model slightly. The removal of the United States from the data also weakened the model somewhat, but remained statistically significant at the .04 level. The reported relationships generally retained the same patterns, but did produce a result indicating that GDP Per Capita may be significant in these relationships. A final test

controlling for democracy using the freedom house scores removed too many cases from the limited database to produce viable results.

Based on this analysis, one could assume that that international investment decisions are not necessarily made with the political environment in mind. Firms seem to value the abilities of the domestic work force and the level of military spending within a state more than levels of corruption, government intrusiveness, and political and civil liberties. The research indicates that firms are investing time, money, and expertise in states that are questionable in terms of an environment that displays marked potential for counterfeiting and possible subversion activities. However, it is very difficult to make assumptions about the psychology of a company and why it may or may not invest in a particular area. While this conclusion is very much only an inference due to the lack of available data directly measuring counterfeiting or subversion activities, the rigor applied by the use of four models is highly suggestive. This model will be especially useful if more precise data, perhaps that which is classified, is utilized to more accurately identify areas in which subversion or counterfeiting may occur.

APPENDIX B: ATTRACTING IT FDI

In recent years China has implemented a wide range of policies to attract FDI, particularly in the IT industry. These policies range from legitimate restructuring and recruitment initiatives, to actions that conflict with international agreements. Cleary, China has successfully promoted its resources and potential to MNEs seeking to decrease factor costs. Although the investment environment differs between the hundreds of separate investment zones within China, there are several key policies that helped the IT industry take hold and flourish.

Imports into China, including ICs, are subject to a 17% Value Added Tax (VAT). Beginning in 2001, China offered a 14% VAT reduction for ICs domestically produced, resulting in an effective VAT of only 3%. A second reduction occurred in localities that waived local VAT revenues. In China, local governments receive 25% of VAT revenues, with the remaining 75% going to the national government. Some local governments refunded their portion to foreign investors. In addition, an effective 0% VAT was granted to MNEs that invested on a large scale and those that engaged in current generation R&D.[238] In March 2004, the US filed a complaint at the World Trade Organization (WTO), claiming the various VAT reductions were discriminatory to other WTO member states. In October 2005, the VAT reductions on ICs were repealed.[239] Although no longer

[238] Chao, Howard and Lawrence Sussman. 2003. "Semiconductor Investment Heats Up in China: A Legal and Tax Guide." Report, O'Melveny & Myers LLP.
[239] World Trade Organization. DISPUTE SETTLEMENT: DISPUTE DS309 China - Value-Added Tax on Integrated Circuits. 11 Aug 2008. <http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds309_e.htm>.

in effect, these policies proved to effective incentives for the budding Chinese IT industry.

MNEs are typically required to pay a 30% national income tax and an additional 3% local income tax. Oftentimes, the national rate is lowered and local rate waived altogether. Additionally, tax holidays are granted to certain MNEs, which grants a two-year full exemption and a further three-years at half the rate thereafter. These exemptions and reductions are increased for technologically advanced firms and those that are engaged in certain R&D activities.[240] Additionally, customs duties - both import and export - are often reduced or waived.[241]

Recruitment policies and campaigns targeting Taiwanese experts and capital have helped China develop a skilled workforce and infrastructure necessary for a mature IT industry. Established Taiwanese businesses are investing in the mainland, moving production functions and managerial know-how in the process.[242]

These policies enacted by the national and local governments have provided many incentives for MNEs to establish a presence in China. These policies were successful to the extent that by 2004, China had become the leading IT exporter in the world.[243]

---

[240] Chao, Howard and Lawrence Sussman. 2003. "Semiconductor Investment Heats Up in China: A Legal and Tax Guide." Report, O'Melveny & Myers LLP.
[241] Chao, Howard & Lawrence Sussman.
[242] Howell, Thomas R., et al. 2003. China's Emerging Semiconductor Industry. Semiconductor Industry Association and Dewey Ballantine LLP.
[243] Chao, Howard & Lawrence Sussman.

Another state that has successfully attracted FDI, with an emphasis on the IT industry, is Ireland.[244] For many years, Ireland lagged behind the rest of Europe in terms economic development. To combat this, Ireland instituted a series of policies in the 1960s designed to spur economic growth. It has today reached parity with the average European GDP. Much of this development is due to the burgeoning IT sector, and the policies enacted to attract this industry. Unlike China, however, Ireland's IT sector is focused primarily on software. Despite this difference, this case is nonetheless instructive of how states can attract FDI.[245]

In the late 1950s, Ireland instituted a zero tax rating on profits gained from manufacturing exports. MNEs thus began to use Ireland as an export platform. Before its entry into the European Union (EU), Irish exports grew substantially. When Ireland became a member of the EU, Ireland had by far the lowest corporate tax rate of any other member state. In 1992, the average effective tax rate for US MNEs was 5.8%. Finland's equivalent rate for US companies was 15.8%, the second lowest in the EU at the time. The result of these policies has been that MNEs can gain a foothold within the EU, from which firms can then export to other EU member states.[246]

Ireland instituted the Industrial Development Agency (IDA) to establish a national model for attracting FDI. Among its successes is attracting Intel Corporation in the late 1980s to manufacture microprocessors in Ireland. The IDA has been instrumental in other ways,

---

[244] Navaretti, Giorgio Barb and Anthony J. Venables. Multinational Firms in the World Economy. Princeton, NJ: Princeton University Press, 2004.
[245] Navaretti, Giorgio Barb and Anthony J. Venables.
[246] Navaretti, Giorgio Barb and Anthony J. Venables.

such as promoting an educational reform that emphasized a technologically-savvy workforce. A concerted effort on the part of the Irish government to attract FDI, and in particular MNEs in the IT sector, has contributed greatly to the economic growth experienced in the past several decades. Both Ireland and China offer cases that illustrate what methods states have at their disposal to attract FDI.[247]

[247] Navaretti, Giorgio Barb and Anthony J. Venables. Multinational Firms in the World Economy. Princeton, NJ: Princeton University Press, 2004.

APPENDIX C: TAX CREDIT BILLS

The House bill is summarized as: “Investment in America Act of 2007 - Amends the Internal Revenue Code to: (1) increase from 12 to 20% the rate of the alternative simplified tax credit for research expenses; (2) make permanent the tax credit for increasing research activities; and (3) repeal the alternative incremental tax credit for research expenses.” The Senate bill is summarized as: “Research Credit Improvement Act of 2007 - Amends the Internal Revenue Code to revise the tax credit for increasing research activities by: (1) phasing-in increases in the alternative simplified tax credit rate through 2009; (2) establishing a 20% alternative simplified tax credit rate in 2010 in lieu of the standard research tax credit rate; (3) increasing the amount of basic and contract research expenses eligible for such tax credit; and (4) making such tax credit permanent.”[248]

[248] H.R. 2138 and S. 2209. 2006-2008. 05 Aug 2008. <washingtonwatch.com>.2006-2008. 05 Aug 2008. <washingtonwatch.com>.

ABOUT THE AUTHORS

Amanda Jokerst graduated magna cum laude from the University of Nebraska at Omaha with a Bachelor's of Political Science in May 2008. She will begin pursuing her J.D. at California's Southwestern Law School in the Fall of 2008

James Martin is a Ph.D. candidate at Creighton University and holds an M.A. in Political Science. He is a part-owner of a media production and graphic design studio, and continues his work there.

Keith Roland graduated from the University of Nebraska-Lincoln with a Master's in Political Science.

Kristen Rodgers graduated from the University of Nebraska-Lincoln with a Bachelor's of Arts and Sciences in Anthropology and Psychology in May 2008. She is currently applying for graduate school, and hopes to obtain a degree in marketing, communication, and advertising.

Erica Tesla graduated from the University of Nebraska at Omaha with a Bachelor's of Arts and Sciences in Physics in August 2008. She continues to work on expanding her photography and freelance writing businesses in Omaha.