Spring 2015
Industry Study

Final Report
Information and Communications Technology

The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) 2015

ABSTRACT: The Information Communications Technology (ICT) industry is vital to the national security of the United States because of its significant economic contribution and because of the increasing reliance upon the Internet for commercial and government activities. The US is currently the global leader in the industry, but it faces significant challenges in innovation, human capital, cybersecurity, and governance. To remain the global ICT leader, the US must meet and overcome these challenges and lead the industry in the emerging trends of cloud computing, mobility, security, and the Internet of Things.

Ms. Tahira Ali, Dept of Homeland Security
COL Abdullah AlShaloob, Royal Saudi Air Force
BG Lior Carmeli, Israeli Defense Forces
COL Paul Craft, US Army
Mr. Mark Crumblish, Lockheed Martin
Mr. Kevin Curry, Dept of the Army
Ms. Christine Jacobs, Dept of State
LTC Stanley Malloy, US Army
Mr. Paul Murphy, Defense Intelligence Agency
Lt Col Richard "Cowboy" Nelson, US Air Force
LTC Christopher O'Connor, US Army
CDR Julia Lopez Slattery, US Navy
Lt Col David Wallis III, US Marine Corps
Lt Col Brandon Wilkerson, US Air Force
Lt Col Patrick Williams, US Air Force
Ms. Maryann Zelenak, Dept of the Air Force

COL David King, PhD, Canadian Forces (Retired), Faculty Lead
COL Richard Altieri, J.D., US Army (Retired), Faculty
Mr. Feza Koprucu, Department of Homeland Security, Faculty
Col Lynne Thompson, EdD, US Air Force (Retired), Faculty

PLACES VISITED

Domestic:

AT&T, Reston VA
CTIA – The Wireless Association, Washington DC
Defense Information Systems Agency, Fort Meade, MD
Department of Homeland Security, Rosslyn, VA
Information Technology Industry Council, Washington DC
International Business Machines, Washington DC
National Cable and Telecommunication Association, Washington DC
National Telecommunications and Information Administration, Washington DC
National Telephone Cooperative Association (Rural Broadband), Washington DC
Software and Information Industry Association, Washington DC
Sprint, Reston, VA
Telecommunications Industry Association, Washington DC
USCYBERCOM, Fort Meade, MD
Verizon, Reston, VA
Apple, Silicon Valley, California
Arista, Silicon Valley, California
Brocade, Silicon Valley, California
Cisco, Silicon Valley, California
Facebook, Silicon Valley, California
Oracle, Silicon Valley, California
Twitter, Silicon Valley, California

International:

Baidu, Beijing, Peoples Republic of China
China Mobile, Beijing, Peoples Republic of China
BDA China Limited, including speakers from:
The US Information Technology Office, Beijing, Peoples Republic of China
The Conference Board in China, Beijing, Peoples Republic of China
Red Pagoda Resources, Beijing, Peoples Republic of China
Huawei Technologies Co, Shenzhen, Peoples Republic of China
ZTE, Shenzhen, Peoples Republic of China
US Consulate, Guangzhou, Peoples Republic of China
American Chamber of Congress in South China, Guangzhou, Peoples Republic of China

The Internet is among the few things humans have built that they don't truly understand. What began as a means of electronic information transmission…has transformed into an omnipresent and endlessly multifaceted outlet for human energy and expression. It is a source for tremendous good and potentially dreadful evil, and we're only just beginning to witness its impact on the world stage.[1]

- Eric Schmidt, Executive Chairman, Google

INTRODUCTION

The Information and Communication Technology (ICT) industry accounts for 4 percent of US GDP and its contribution to other segments has been responsible for as much as 7 percent of GDP.[2] The compound benefits of ICT are also responsible for as much as 20 percent of GDP growth since 1995, adding more than $2 trillion in real terms.[3] This trend is highly likely to continue. Today there are 10 billion devices connected to the Internet. This number is expected to increase to 30-50 billion by 2020.[4] This proliferation of smart, connected devices is called the Internet of Things (IOT). IOT has the potential to provide an annual economic impact of $2.7 trillion to $6.2 trillion by 2025.[5]

As stated in the 2015 National Security Strategy, "The American economy is an engine for global economic growth and a source of stability for the international system… [and] it underwrites our military strength and diplomatic influence. A strong economy, combined with a prominent US presence in the global financial system, creates opportunities to advance our security."[6] The importance of the ICT industry to the US economy is clear and the industry's importance to national security is increasing. The ICT industry is inextricably linked to cybersecurity, an issue that is critical to government, economy, and individual citizens.

To assess the ICT industry's health and its economic and national security impact, the seminar analyzed the industry using a variety of tools including Porter's Five Forces Model, the Structure-Conduct-Performance framework, strategic financial analysis, industry and trade association reports, and field studies in the US and China. This analysis is summarized in Section III and Appendix B. Overall, we found that the ICT industry remains dynamic and healthy. In addition to its significant GDP contribution, the industry employs 4.35 million people[7]. The industry continues to be a hub of innovation, regularly accounting for 35-40 percent of all patents.[8] There is robust competition in most of the industry segments. The relatively low entry barriers continue to decline as the services components of the industry become more important and as cloud computing transforms fixed costs to variable costs.

The ICT industry does face challenges. During our field studies, industry stakeholders expressed concern about cybersecurity, human capital, innovation, and governance. For the US ICT industry to remain the global leader, industry stakeholders need to take action to overcome these challenges. These challenges are discussed in Section IV and we offer recommendations to address them in Section VI.

The industry's outlook is highly positive based on the strength of its firms, the quality of its people, and significant future market opportunities. If the US can address the above-mentioned challenges, the industry's outlook is excellent. The seminar noted several trends that will be particularly relevant to the industry over the next several years. These include mobility, cloud computing, security, and global competition, which are discussed in Section V.

THE INDUSTRY DEFINED

The ICT industry is difficult to define because information technology (IT) has become so ubiquitous. For the purpose of our analysis, the industry is defined based on thirteen North American Industry Classification System (NAICS) codes from the most recent Census Bureau Economic Census (see Table 1). These NAICS codes were selected in an effort to define the industry broadly enough to draw meaningful conclusions about the ICT industry and its ability to meet national security needs. The seminar grouped similar industry segments into four categories to facilitate analysis.

Category	NAICS	NAICS title	Descriptor	Revenue[9]
Manufacturing	33411	Computer & Peripheral Equipment Manufacturing		$36.8B
	33421	Telephone Apparatus Manufacturing	Telecom Networking Equipment Manufacturing	$8.2B
	33422	Radio/Television Broadcasting & Wireless Communications Equipment Manufacturing		$33.8B
	33461	Manufacturing and Reproducing Magnetic and Optical Media	Recordable media manufacturing	$2.0B
Communications Services	51521	Cable and Other Subscription Programming	Cable Networks	$56.0B
	51711	Wired Telecommunications Carriers	Cable Providers	$84.9B
	51711	Wired Telecommunications Carriers	Wired Telecommunications Carriers	$169.5B
	51711	Wired Telecommunications Carriers	Internet Service Providers	$92.6B
	51711	Wired Telecommunications Carriers	Voice Over Internet Protocol Providers (VoIP)	$5.6B
	5172	Wireless Telecommunications Carriers		$242.1B
	51741	Satellite Telecommunications		$6.7B
	51791	Telecommunications Resellers		$13.2B
Software and Internet Publishing	51121	Software Publishers		$196B
	51913	Internet Publishing and Broadcasting and Web Search Portals	Search Engines	$60B
Computer Services	51821	Data Processing, Hosting, and Related Services	Data Processing & Hosting Services	$118B
	54151	Computer Systems Design and Related Services	IT Consulting in the US	$354B

Table 1. Industry Definition, Description and 2014 Revenues

CURRENT CONDITION

The ICT industry has experienced significant evolution over the past five years, leading to a rapidly expanding market. As the services components of most industry segments have increased in size, importance, and revenue generation, the barriers to entry have consistently lowered. The

following section provides a structure/conduct/performance (SCP) analysis of industry segments as well as firm analysis commentary, designed to provide insight into the health of the industry and its component firms. For each of the industry categories, one segment was selected as an industry proxy for purposes of analysis and discussion. A summary of the strategic financial analysis on the top firms in each segment is included in Appendix B.

Manufacturing (NAICS 33411, 33421, 33422, 33461)

The Communication Equipment Manufacturing segment (NAICS 33422) serves as the proxy for Manufacturing. This segment manufactures broadcasting and other wireless communication equipment. Annual segment revenues grew 1.5 percent annually over the past five years and are expected to increase to 2.4 percent per year through 2020.[10] The segment employs 71,000 people with average compensation of $97,000 per person.[11] Average profit margins, measured as earnings before interest and taxes (EBIT), are 4.9 percent. These margins have been driven down due to competition from offshore manufacturers.

The top three firms in this segment, Cisco, Harris Corp, and Alcatel-Lucent, account for 41 percent of revenue.[12] The rest of the market is made up of 765 companies which provide differentiated offerings.[13] Competition within the industry is based on price, quality, and service.[14] Firms are differentiating in an attempt to gain pricing power and recover shrinking margins. The firms have adequate liquidity to cover debt service. Capital intensity is low but firms must invest significantly in R&D to innovate. Overall, the health of leading firms, and the sector, may be of concern. The average firm struggles to earn its cost of capital; only Cisco has consistently done so in the last five years.

The health of the Communications Equipment Manufacturing segment is improving due to a rebound in domestic spending after the recession, new product offerings, and the growing number of mobile connections which drives demand for equipment in this segment. However, the segment continues to face threats from offshore competition. Additionally, some firms in the segment face threats due to overall shifts in the ICT industry.[15]

The future of the other segments in Manufacturing (NAICS 33411, 33421 and 33461) do not look as promising. Revenue in each of these sectors is expected to shrink in the next five years due to competition from offshore firms and overall changes in the ICT industry (e.g., consumer demand moving from desktop computers to mobile devices and consumer preference switching to streaming services).[16]

Communication Services (NAICS 51521, 51711, 51721, 51741, 51791)

The Wireless Telecommunications industry (NAICS 51721) serves as the proxy for Communication Services. This segment operates and maintains switching and transmission facilities to provide direct communication through radio-based cellular networks.[17] Industry services include cellular mobile phone services, paging services, wireless Internet access, and wireless video services. Annual segment revenue growth averaged 2.2 percent over the past five years and is expected to grow at the same rate through 2020.[18] The segment employs 260,000 people with average compensation of $66,000 per person. Profit margins are 25 percent. The top four firms, Verizon, AT&T, Sprint, and T-Mobile account for over 90 percent of the total market with Verizon and AT&T the clear market leaders.[19]

The wireless industry, a key driver of the Communications Services category, is a highly competitive environment where high capital requirements depress profitability and limit shareholder returns. Analysis of this market indicates that it is unlikely to sustain the four current

players. Sprint's current operating model is not sustainable, losing money on every customer and generating negative financial returns, while continuously restructuring its debt just to stay afloat.

While AT&T and Verizon may benefit from a considerable upside in the wireless market space over the next five years, this will likely be off-set by a slowdown in their wired revenues. Wireless businesses at both AT&T and Verizon rely upon their wired infrastructure to deliver service, so there is considerable synergy. In the wired space, neither firm can extract profit from their position due to its capital intensive requirements. Verizon is in better financial shape because it has been able to slow its capital expenditures as it is further along in its infrastructure build out. AT&T continues to invest to catch up resulting in in substantial downward pressures in shareholder returns. Uncertainty surrounding the recent Federal Communication Commission (FCC) Open Internet Order (i.e., Net Neutrality) may also be contributing to the overall slowing of capital expenditures focused on infrastructure build-out.

Software and Internet Publishing (NAICS 51121, 51913)

The Software Publishing segment (NAICS 51121) serves as the proxy for Software and Internet Publishing. This segment provides design, development and publishing of software/firmware/middleware for computers and mobile phones. Software types include system, application, database and custom software (including security). Annual segment revenue growth was 4 percent over the past five years and is expected to decrease to 3 percent by 2020.[20] The segment employs 294,000 people with average compensation of $158,000 per person. Profit margins are 22 percent. The top three firms, Microsoft, Oracle, and IBM account for 34 percent of the total market. The industry is highly competitive with over 6800 companies that offer specialty solutions.[21] Capital intensity is low but firms must invest significantly in R&D and human capital to innovate and compete successfully.

Business models in this industry are shifting from the traditional software publishing model toward software delivered online, which is changing the competitive landscape and may drive consolidation within the industry.[22] As the industry evolves, firms are investing in software-as-a-service (SaaS) and cloud computing as mobile platform adoption rapidly increases. The industry is healthy with plenty of liquidity to cover debt service. The average firm earns more than its cost of capital and the top three firms in this segment are realizing profit margins significantly above the segment average. This segment is healthy and has a positive outlook over the next five years as does the Internet Publishing segment.

Computer Services (NAICS 51821, 54151)

The IT Consulting segment (NAICS 54151) serves as the proxy for Computer Services. This segment includes "writing, testing and supporting custom software; planning and designing integrated hardware, software and communication infrastructure; and on-site management of computer systems and data processing facilities."[23] Annual segment revenues grew at 3.6 percent over the past five years and are expected to increase to 4.0 percent by 2019.[24] The segment employs 1.8 million people with average compensation of $83,000 per person.[25] Average profit margins are 13.2 percent. The top four firms in this highly competitive segment account for only 13.3 percent of the total market. Within this industry International Business Machines and EMC focus on a combination of products and services while Hewlett-Packard and Accenture focus on services alone. The rest of the market is diverse consisting of 442,000 companies offering specialty solutions.[26] Capital intensity is low and firms do not currently need to invest significantly in R&D to innovate.

This industry segment is highly competitive with a multitude of niche players that specialize in either products or services, or a combination of the two. Competition is based on price, quality of service, expertise, and the breadth of service offerings.[27] The industry is evolving as more investment is made in software services and as mobile platform consumption rapidly increases.[28] The industry is in good health with plenty of liquidity to cover debt service. The average firm earns more than its cost of capital; however, in each specialization area, the market share leading player performs best. IBM is outperforming EMC and Accenture is outperforming H-P on profitability and ROA. The top four firms by market share are capturing high profit margins in this segment. While the margins are high, all four companies have been unable to increase those margins in recent years.

CHALLENGES

The US is moving into a realm of increasing uncertainty within the ICT domain. We are confronted with wicked problems that will continue to challenge us in this interconnected and global community. These challenges are constantly evolving and moving at the speed of technology and in some cases the US is responding at the speed of bureaucracy. Our analysis of the ICT industry identified four pervasive challenges: innovation, human capital, cybersecurity, and governance. To remain the global ICT leader, the US must address and overcome these challenges. This is difficult because these areas have interdependencies that increase the complexity of the challenges. We explore each of these challenges in more detail in this section. Recommendations to address these challenges are provided in Section VI.

Technology Advancement

What is America's true potential as an economic power? Our economy has had its bumps and bruises over our history and we have always bounced back quickly – until recently that is. The "Great Recession" of 2008 has continued to linger much longer than past economic downturns.[29] The current expansion (recovery) period has lasted 60 months and by most measures is lagging significantly behind all previous expansion periods since WWII.[30] At the current pace, we are not expected to reach our potential until 2017 or 2018.[31] How can we realize that potential and continue to raise the bar to new heights? We face numerous challenges as we continue forward into the 21st century. The honorable Mr. Frank Kendal stated that he believed that we were losing our technological advantage to China if we had not done so already.[32] We, as a nation, have been able to leverage technology to supplement our fighting force and use it as a force multiplier. If we are going to continue to have this advantage we must continue to invest in research and development and also in our human capital. One of our key national security interests, which is delineated in the 2015 National Security Strategy, is "a strong, innovative, and growing US economy in an open international economic system that promotes opportunity and prosperity."[33] In addition to this, President Obama stated, "Scientific discovery and technological innovation empower American leadership with a competitive edge that secures our military advantage, propels our economy, and improves the human condition."[34] During our visits with ICT firms, we continued to hear similar themes regarding innovation. Every company valued engineering and technological innovation and identified it as a strategic core competency.[35] Some talked of an engineering-driven culture and identifying "entrepreneurs in residence" programs to stimulate creativity.[36] Others talked about "moving fast and breaking things," meaning that you should not be afraid to come up with new ideas and pushing ahead with them.[37] You have to take risk if you are going to truly innovate. Humans tend to think of things in terms of being linear, but technological advancements are

moving in exponential terms.[38] We are challenged with sequestration and the forced reduction in our government budgets; increasing mandatory expenditures for Medicare/Medicaid and Social Security; dwindling enrollments in STEM education; the need for immigration reform and visas for highly skilled workers; and the need for tax reforms on corporate taxes and the research and development tax credit.[39] We are going to have to figure out how to resolve these challenges and capability gaps if we are going to continue to prosper as a nation and ensure our national security in the 21st century and beyond. The following essay will discuss the impact of ICT on the economy and its importance to national security.

Innovation in ICT

The ICT industry permeates through all of the business environments and is identified as a significant enabler to economic growth.[40] Stephen Ezell mentions in one of his op-eds that that ICT acts as "super capital" because it enables the workforce to work more efficiently and it makes physical capital more productive.[41] US firms lead the world in the adoption of ICT.[42] It has been shown that US firms get more of a benefit out of ICT investment than many of their foreign competitors.[43] It is not just the investment in ICT, but it is the application of it to improve business processes that have resulted in US firms gaining the most benefit from these technologies.[44] The ICT industry has been a leader in innovation and investing in research and development compared to other industries and segments. The ICT industry as a whole averages around eight percent of sales revenue spent on R&D in 2013 (Software and Internet: 13 percent; Computing and Electronics: 8 percent; Telecom: 1.5 percent).[45] The average for all other industries is hovering around 3 to 5 percent as a percentage of sales.[46] A look at a select few leaders within the ICT industry shows the following spent on R&D in 2013/14 (percentages of sales in parentheses): IBM: $6.226B (15.5); Microsoft: $11.381B (19); Cisco: $6.294B (13.4); Oracle: $5.151B (16.7).[47] The Bureau of Economic Analysis (BEA) started accounting for R&D as an investment in 2006 by reporting the Research and Development Satellite Account.[48] They have analyzed the impact that R&D has had on the overall GDP historically from 1959 through 2007. The consensus is that GDP would have been reported higher overall throughout those years if R&D would have been reported as an investment.[49] In 2007 alone, the additional growth to the GDP would have been approximately $300 billion.[50] On average, R&D would have contributed an additional 0.20 percent to the 2.9 percent average growth rate between 2002 and 2007.[51]

Across the broad spectrum of industries that contribute to our nation's GDP, the ICT industry is among the more significant contributors to real GDP.[52] Only pharmaceuticals and medicine manufacturing industries have recently contributed more as a percentage of GDP resulting from R&D investment.[53] In 2009, ICT firms contributed 7.1 percent of the US GDP or approximately $1 trillion.[54] This includes the direct contribution from ICT firms as well as the indirect benefits other segments derive from the ICT industry.[55] ICT provides enabling technologies that can be applied to every other industry; therefore, innovation within ICT not only results in growth for the ICT industry, but creates spillover to other industries contributing to their economic growth as well.[56] Robert Shapiro and Aparna Mathur of the Bureau of Economic Analysis found, "In the 1990s, investment in ICT by other industries grew 10 times faster than their investments in any other inputs."[57]

When you see growth and increases in productivity within a corporation or a country, it is mostly likely the result of acquiring new knowledge or innovation with respect to processes or products. Since the 1990s, ICT has been the dominant force behind those innovations.[58] Innovations in science and technology have shown to be the key determinants in a nation's

economic growth.[59] Research performed by Nobel laureate Robert Solow in the 1950s established that technology innovation is a dominant factor in economic growth.[60] He showed that economic growth could not be accounted for by increases in capital and labor alone, and the unaccounted portion was attributed to technological innovation.[61] Solow further discovered through his research that 30 to 40 percent of economic growth within the US during the 20th century can be directly attributed to innovation.[62] The role of ICT innovation has shown to have accounted for 28 percent of US economic growth from 1995 to 2001, and another 44 percent could be explained by the capital investments and organizational changes by firms in response to those innovations.[63] The fact is that ICT is an enabler that permeates every industry and results in positive economic effects.[64] Also known as spillover effect, ICT innovations result in organizational and process changes within other industries that lead to greater efficiencies and future economic growth.[65]

Technology is a key component to national security in today's interconnected and digital world. There are five broad areas of technology that have an impact on national security: biotechnology and medicine; robotics and autonomous systems; information and communications technology; nanotechnology; and energy technology.[66] It can be argued that ICT, as stated previously in this essay, contributes to advancements in all the areas of technology. ICT specifically is supporting cognitive sciences and advanced decision support tools along with the possibility of quantum computing in the not too distant future.[67] R&D investment in ICT was also of special importance in resolving national defense problems such as calculating nuclear testing performance, cryptanalysis, cybersecurity, and weather modeling.[68] These technological advances could result in revolutionary changes in how we conduct national defense and spillover into commercial products, applications, and processes that will provide increased productivity throughout the economy.

The realm of cybersecurity and the protection of our privacy, our networks, and our critical infrastructure will depend on our ability to maintain our technological advantage over the rest of the world. As we continue to demand more mobility in our IT systems (e.g. smartphones, tablets, wearable devices, etc.) and we move to a cloud-based computing architecture, we will be even more reliant on improved cybersecurity to protect our privacy and our security. In order to do this we need to look at innovation as a strategic imperative for our nation.

Human Capital: Strategic Fuel for the National Economic Engine

"We cannot sustain an economy based on innovation unless we have citizens well educated in math, science, and engineering. If we fail at this, we won't be able to compete in the global economy. How strong the country is twenty years from now will be largely driven by this issue." (Bill Gates).[69] The ICT industry is the nation's digital nervous system, the electronic interstate that has been the engine of US GDP over the past five years. GDP has two drivers: human capital and productivity. Human capital includes the education and training required by the marketplace. Appropriately developed human capital that is available in sufficient quantity stimulates GDP growth through the efficient application of specific skillsets. Human capital is the source of the innovation that creates economic value and fuels the nation's economic engine. The US's human capital problem has two dimensions. The first concern is an insufficient quantity of domestically produced Science, Technology, Engineering, and Mathematics (STEM) graduates. The second problem is the insufficient number of skilled immigrants (H1-B visa recipients, a 3-year work visa issued by the US government for specific foreign workers) to cover the gap between the needs of US industry and the supply of US educational institutions.

There are national security implications in the nation's failure to produce a sufficient quality and quantity of human capital. Microsoft Corporate Vice President for Research, Mr. Peter Lee, stated in testimony before Congress:

> The Bureau of Labor Statistics estimates that between 2010 and 2020, there will be at least 1.2 million job openings in computing professions that require at least a bachelor's degree (on average 120,000 per year) and that in 2020 half of the over 9 million STEM jobs will be in computing. Yet in 2010, only about 60,000 bachelors, masters, and Ph.D. degrees were awarded in computer science.[70]

The ICT industry has consistently failed to find the quantity and quality of STEM graduates that it demands. The nation's education system has not met the requirements of the ICT industry. Roughly 34 percent of college freshman in 2009 indicated that they desired to complete a STEM course load. Unfortunately, only 30 percent of those who chose a STEM course as a freshman graduated with a STEM degree within five years.[71] The inability of the US to meet the requirements of its key industries is demonstrated in a global comparison of bachelor's degrees awarded in 2008. Globally, China produces 23 percent of all STEM undergraduates, the EU produces 19 percent, and the US only produces 10 percent.[72] It should be noted that US STEM production also includes foreign students. Foreign students dominate the STEM postgraduate fields; over 50 percent of Doctoral degrees in Engineering, Physics, Computer Science and Economics are awarded to foreign students.[73] There are benefits to having foreign students as part of the US educational institutions' contribution to the STEM workforce; the problem is in keeping that human capital investment in the US and convincing them to become citizens.

In the seminar's trip to China, it was readily apparent that the sheer scale of the education system in a nation of 1.3 billion people provided an immense amount of STEM-trained human capital. However, there were indicators that the education system in China still lacked the ability to imbue its graduates with the intangible elements that form the foundation of innovation within the US ICT industry. Additionally, the transition to an education system in which students were paying tuition has resulted in an extremely competitive testing regimen for Chinese youth and raised graduates' compensation expectations. It was insightful to see how many of the key leaders in China's ICT industry had received tertiary education within the US. However, the potential issues with China's education system does not release the US from the need to provide STEM-trained graduates in sufficient quantities to sustain GDP growth. It is important that the US raises the aggregate level (in terms of quality) of its STEM education. Greenwald and Stiglitz (2012) have determined that "higher aggregate education results in greater human capital accumulation" and "the resulting human capital accumulation is a critical element in both developing the innovations on which productivity growth depend and disseminating them as workers move within enterprises and across sectors."[74] These spill-over effects indicate the importance of human capital accumulation. Higher skills and higher levels of human capital, unlike physical capital, do not depreciate. Once the stocks are built up, they remain in the economy even as people move from one firm to the next."[75]

The tertiary education institutions appear to be responding adequately to human capital markets. That does not appear to be the case at the primary and secondary education levels. US primary and secondary education institutions are predominantly state-regulated monopoly providers to the human capital market. Industry has determined that the organizations responsible for producing the human capital for the economy are not responsive to market demands, are not efficient, and do not rapidly respond to market incentives. The ICT industry has been asking for federal government support to meet its needs for STEM graduates since at least the mid 1990's.

However, due to US Constitutional authority codified in the 10th Amendment, states are responsible for education leaving the federal government with a role of coaxing and incentivizing through funding, grants, and awards and trying to standardize education through legislative and/or executive branch initiatives.

The ICT industry would also like the federal government to increase the number of skilled worker (H1-B) visas. The H1-B visa was designed as a three year work visa to be awarded to 65,000 foreign workers with critical skills on an annual basis. However, as the ICT industry has expanded it is outstripping the supply of both domestic STEM graduates and the industry's portion of the 65,000 annual H1-B visa applicants.

Cybersecurity: Information Sharing, Liability Protection, and Critical Infrastructure

An adequate level of cybersecurity has become essential to the dynamic and continually evolving personal, business, and government communications and data processing across the ICT industry. A significant challenge is to be found in the definition of "adequate" and determining what constitutes "enough" cybersecurity. Equally challenging is the determination of who should be held accountable and resourced to provide "adequate" cybersecurity. The answer: it depends on what one is defending, but will require the commitment of both government and private industry to succeed. In the interest of national security, government must have <u>at least</u> enough cybersecurity to protect and defend the nation, including critical infrastructure. Private industry, in the interest of protecting data, must have <u>at most</u> enough cybersecurity to fit within their business plan and to ensure their sustainment and future growth in the event of a cyber-intrusion. Both share a common goal of assured access to information and data, and confidence that data integrity is maintained and kept secure. Three critical areas have been identified: information sharing and transparency, liability protection, and government regulation. The end-state is national cybersecurity that has as its primary components *adequate cybersecurity in support of national security interests including critical infrastructure (for government), and adequate cybersecurity to ensure market revenues sufficiently exceed the costs of providing the service (for private industry).* Both of these demand assured access to information and data, coupled with confidence in the integrity of that data. Without improved cybersecurity, we may witness a slowing of the digital economy, which has negative implications for economic growth and national security.

<u>Information Sharing</u>. The suggestion that government and private industry should work to collaborate and share information about cyber threats is about more than being *friendly* - it is a necessity. The Federal Bureau of Investigation's (FBI) Cyber Division Section Chief recently noted that "contrary to pubic belief, we [FBI] can't see it all and a lot of intelligence and evidence lies on the private networks. Cyber is like no other threat we face and we can't do our job without private sector help."[76] This is a partnership. To be effective, information must flow between government and private industry, and must be at the speed of necessity.

The framework for increased information sharing exists in some areas, and is being created in others, if only as a reaction to recent high profile cyber attacks within the US. Within the US government, the Department of Homeland Security (DHS) is responsible for addressing protection of critical infrastructure from physical and cyber threats.[77] Sharing information about malicious cyber activity is key to this mission. DHS runs the Communications Information Sharing and Analysis Center (ISAC) which includes over 66 voluntary members of the ICT industry in its operations. Indeed, the recently signed National Cybersecurity Protection Act (NCPA) designated

the National Cybersecurity and Communications Integration Center (NCCIC) as a "federal civilian interface with the private sector for purposes of cybersecurity information sharing."[78] As with the ISAC, coordination with the NCCIC and NCC watch is voluntary for private industry.

President Obama recently signed an Executive Order (EO) that outlines his administration's intention to begin forming information sharing and analysis organizations (ISAO) and has included ISAOs in a draft legislative proposal. Designed to complement the existing ISACs, the ISAOs are intended to be "more flexible and adaptive to the threat environment than the existing, segment-specific information sharing and analysis centers."[79] This EO sets the stage for movement of existing cybersecurity legislation, currently awaiting Congressional action.

The Cyber Threat Intelligence Integration Center, created under authorities granted to the Director of National Intelligence (DNI), is another positive sign. Yet it will be critical that such new organizations do not dilute the already limited resources of lead agencies like DHS in an effort to gain more eyes on the cybersecurity threat.[80] As DHS is chronically underfunded, it may prove beneficial to better resource DHS in their role as the designated national security lead for protecting the country from cyber threats, and to strengthen their perceived value-added to private industry as a cybersecurity leader. Future cybersecurity strategy must continue to emphasize the role of key players, like DHS, in order to avoid fracturing resources and effort.

Liability protection. The recently signed Information Sharing EO includes language that acknowledges the concern of private industry on the need for liability protection. Many sources in industry note that the administration's support for liability protection is "necessary, but it is not sufficient" stressing that liability protection must come in the form of "iron clad protections" of a law.[81] Legislation put forth by the Executive Branch aims to address this pressing concern from industry.

There is support from the intelligence community (IC) for steps that bring private industry to the information sharing table. Admiral Mike Rogers, Director of the National Security Agency (DIRNSA), testified to the House Armed Service Committee his support for increased transparency from the IC on info sharing and NSA objectives, noting that the IC does not have the authority, nor do they wish to be in the private networks. They want to collaborate and share in a true partnership with private industry.[82]

Critical Infrastructure

> *Electricity is the foundation for America's economic success. Our digital economy, our national security, and our daily lives are highly dependent on reliable, safe, abundant, affordable, and secure electricity.*[83]

The February 2013 Presidential Policy Directive (PPD) 21 called for "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure" and tasked DHS to provide strategic guidance and primacy for implementation of this policy.[84] In turn, DHS identified 16 segments that met the criteria of critical infrastructure.[85] While each segment certainly has an identified requirement for cybersecurity, it can be argued that the *primus inter pares* is the defense of the electric grid. Of our many critical infrastructures, it is perhaps our electric infrastructure that has the greatest potential for mass disruption and would allow any foe or mal-actor to see the greatest disruption to our way of life. On November 20, 2014, Admiral Rogers speaking in his role as both the Director of the National Security Agency and Commander of US Cyber Command stated to the House Intelligence Committee that "China and 'one or two'

other countries have the power to shut down the US electric grid with cyber attacks."[86] He added "multiple nation states are seeking to acquire the same kinds of cyber capabilities possessed by China."[87]

The response required to repair the grid in event of a cyber attack would require a substantial whole-of-government response. The loss of power to 8.5 million people due to Super Storm Sandy on October 29, 2012, while not a cyber attack, provides insight into the possible national security implications of such a devastating loss of electricity.[88] The response to get the power turned back was an inter-state and a whole-of-government effort. For example, the US Air Force flew bucket trucks in from California into the most affected areas in New York and New Jersey.[89] In total, 16,176 active duty and National Guard personnel responded to the crisis,[90] in addition to the 57,000 utility workers that worked to get the power turned back on.[91] The impacts of Super Storm Sandy give anyone studying national security pause when considering the impacts of a prolonged power outage.

An initiative that has a direct impact on the ICT industry is the effort called "smart grid." According to the US Department of Energy (DOE), the smart grid is the "class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation."[92] The smart grid will be "made possible by two-way communication technology and computer processing that has been used for decades in other industries."[93] The smart grid will integrate the different forms of electric generation from wind and solar to our current forms of coal, natural gas, etc.[94] In order to make the smart grid work, electric companies will have to emplace sensors that have the ability for two way communications with those sensors located from the each home all the way through the electric grid network.[95] The cyber threat to this investment cannot be overlooked. A 2011 New York Times article quotes the Electric Power Research Institute (EPRI) as saying that the cost of the smart grid will be somewhere between, $338 to $476 billion over the next 20 years.[96] The cyber risk to the future electric grid cannot be overstated.

Cybersecurity regulations will undoubtedly have a significant impact on not only the solutions and services implemented by ICT firms, but also on future compliance, national security, and bottom line profits impacting the future health of the industry. The government must demonstrate its willingness to be transparent in its objectives in partnering with private industry, especially in the wake of the Snowden revelations. Private industry must expect that the government will "share information almost immediately with some exceptions"[97] in order to mitigate damage to the private sector. Yet, private industry must be willing to demonstrate its willingness to collaborate in turn. A former cybersecurity adviser to both President Bush and President Obama warned private industry that "if we don't start telling the government that we are doing things…the government is going to continue to look down the road of 'how do we regulate?' They'll start focusing on critical infrastructure first. Then they'll start looking at the economic world – and not just financial services companies."[98]

Transparency and information sharing, protected collaboration, balanced regulation, and adoption of recognized standards are necessary to create a national strategy for cybersecurity in a world where no one entity can secure all. As noted in the 2015 NSS, "Collective action is needed to assure access to the shared spaces – [to include] cyber…where the dangerous behaviors of some threaten us all."[99] The strategy must direct the government to secure infrastructure that is critical to national security and coordinate with those industries that build, own, or operate the critical infrastructure. The strategy must also support, clearly encourage, and enable private industry partnership while allowing private industry freedom to evolve as their respective industries dictate.

To that end, the US should adopt a cybersecurity policy that has as its objective: *adequate cybersecurity for government (in support of national security interests) and private industry (in support of data security) which provides assured access to information and data, coupled with confidence in the integrity of that data.*

Governance

There are two major challenges the US Government faces with regard to governing the ICT industry: ensuring continued exemplary economic growth and ensuring national security. To *ensure the future economic viability of the ICT industry,* the government role should be ensuring that companies do not exploit their market power to the detriment of efficient competition. This includes managing spectrum sharing and reallocation, promoting competition between service providers, and enabling Net Neutrality without stifling commercial investment. It also includes determining the direction of the Internet Corporation for Assigned Names and Numbers (ICANN) after the current Department of Commerce contracts expire and addressing the rapid growth of the Internet of Things (IOT) which entails both a security and privacy challenge.

Ensuring strong federal ICT-focused security requires updating legislation and sustaining resourcing. Updated legislation should focus on modernizing ICT security standards for federal information systems and for commercial information systems where markets are too slow in reaction to cyber threats/attacks. The focus of security standards should include: wireline/wireless infrastructure, architecture, cloud/data storage, software/hardware, computing power, and supply chain management.

Heavy regulation hinders growth, stagnates innovation, sours the spirit of business competition, provides advantage to the inefficient, and limits consumer choice. Heavy regulation could weaken the health of the ICT industry and hurt US competition in international markets. This would impact the greatest economic engine our economy has ever known – the commercial Internet. As our dependence on ICT products and services grows exponentially, we may see increased regulation targeted at the overall ICT industry. This may be beginning to happen with regulations dealing with cybersecurity, Net Neutrality, and spectrum management.

Light regulation has allowed technology and business pioneers to create the extensive Internet capabilities we enjoy today. Light regulation continues to be adequate for the industry. There is a definitive need for some regulation to maintain or enhance security and to ensure equal access to both domestic and international markets through international trade agreements and trade agreement enforcement. But these regulations should be limited

Legislation is another consideration. A complicating factor is that legislation related to ICT has not kept pace with rapid advances in the industry. Much of the base ICT legislation was originally written in 1934 (Telecommunication's Act) and the original information systems security legislation (Federal Information Systems Management Act) was originally written in the 1990s and early 2000s. Lagging legislation created security gaps as the Internet developed so quickly. Congress was slow, or unable, to pass legislation so President Obama addressed the security gaps with Executive Orders (EO) and Presidential Policy Directives (PPD). These EOs and PPDs lack the required resources to be robustly carried out, so legislation is still necessary. To address Internet security, Congress must provide updated legislation and the requisite resources to enable and enforce the law.

The key to solving the governance challenges is to arrive at an acceptable balance between national security and economic growth. Over regulating the ICT industry will actually hamper its

ability to remain economically viable; the US government must find a way to provide the proper level of governance to achieve overall balanced success. Our view is that regulation should not be anticipatory; it is needed primarily to deal with market failure that is demonstrated to have materially diminished competitive market outcomes. The following sections discuss specific governance challenges and factors that should be considered to address them.

Federal Information System Security and Critical Infrastructure

An example of out-of-date US Code is Title 44, the Federal Information Systems Management Act (FISMA), which has not kept up with rapidly changing information technology security standards and definitions.[100] Because the law was originally written in 2002, prior to the enlargement of the Internet and cybersecurity, its policies and statutes do not align with the much more efficient and operationally accepted standards and practices for IT security. The law's manual processes for security compliance made sense when introduced due to a limited number of IT systems in a few large federal data centers. With the explosion of the Internet, data centers, and IT systems and software in those centers, the older manual process became overbearing and compliance to those standards lagged, creating major cybersecurity shortfalls.

Securing the supply chain

American ICT manufacturing has been moving overseas, particularly manufacturing of microprocessors (MP), the basic physical "DNA" building block of ICT hardware. Offshoring has been the result of two significant trends, *explosive growth in capital cost in MP plant construction, and rising Chinese dominance in the MP value chain.* Rising cybersecurity threats emerging from China suggest that a substantial portion of MP-based systems may be compromised, or may be compromised in the future. Additionally, the US dependence upon Chinese MP manufacturing presents serious risks of supply chain shortages, or possibly a complete supply hold up, in the event of a Sino-US confrontation. This is a strategic liability for the US.

IT acquisition reform

It is well documented that technological advances in IT systems and capabilities have outpaced the federal government's ability to develop and acquire it in a timely manner. A new technology could take more than seven years to go from a stated requirement to being put into the hands of the military, by which time the technology has often been obsolete. A number of policy and legislative initiatives have been undertaken to solve the problem. Most recently, Congress passed the Federal Information Technology and Acquisition Reform Act (FITARA) in December, 2014 as part of the 2015 National Defense Authorization Act. The legislation pushes for CIOs to have a greater role in programming, budgeting and decision-making related to IT at their agencies and calls for them to approve all agency IT or IT service deals before a contract can be signed.[101] Critics of the legislation argue that it failed to include systemic reforms needed to address the central issues such as multiple CIOs in agencies and departments.[102] The seminar heard similar criticisms from ICT industry executives who asserted that the federal government's $80 billion per year IT budget should be more than adequate to fully recapitalize federal IT systems within a few years.[103]

Net Neutrality

Net Neutrality is a critical policy discussion that has implications across all ICT sectors. In February, 2015 the Federal Communications Commission issued an Open Internet Order, adopting rules "designed to protect free expression and innovation on the Internet and promote investment in the nation's broadband networks. The Open Internet rules are grounded in the strongest possible legal foundation by relying on multiple sources of authority, including: Title II of the Communications Act and Section 706 of the Telecommunications Act of 1996."[104] Based on our interactions with industry and trade associations, we expect there will be challenges to the legality of the FCC's decision. Ultimately, how the US government regulates the Internet will have dramatic impacts on the industry.

Compared to the rest of the world, US broadband companies deliver better overall value, better penetration, more choices, and invest 60 percent more per capita than the Organisation for Economic Co-operation and Development (OECD) average to continuously improve broadband performance and penetration. With very limited regulation, it has become one of the greatest success stories in the history of commerce. There does not appear to be any substantive evidence of consumer harm, anti-competitive behavior, or other significant market failures that would require government regulation. Based on this assessment, it appears that the FCC's designation of the Internet as a public utility was preemptive and premature. The FCC's rules may limit private investment in broadband infrastructure which would ultimately hurt US innovation and leadership in the ICT industry.

The Future of ICANN

The US Government's desire is to have the management of the Internet domain name system (DNS) transferred from the National Telecommunications and Information Administration (NTIA) at the Department of Commerce (DOC) and the Internet Corporation for Assigned Names and Numbers (ICANN) to a non-governmental multi-stakeholder entity. The Obama Administration has made it clear that the US will not support a DNS system under the control of another national government or the United Nations. The ICANN governance group looking at options has yet to make a proposal that has met with any approval, so at this point the default course of action is to maintain the status quo. The current NTIA contracts with ICANN for DNS management are set to expire on September 30 of this year, but they can be extended through September, 2019 if needed to provide another four years for the ICANN group to come up with an acceptable multi-stakeholder model to manage the DNS system in the future.

INDUSTRY OUTLOOK

This section discusses significant trends shaping the ICT industry today and into the future. These include cloud computing, analytics, mobile devices, social media and the Internet of Things (IOT). These trends are overshadowed by the US economic national security concern of losing the ICT market to non-democratic countries and non-market based governance models, democratic and undemocratic.

The Future of the Cloud -- Data Localization and Storage

As discussed earlier, security is a pervasive concern within the ICT industry. Several sectors within the industry are trying to define a workable information storage and processing

infrastructure, the "cloud," that would help mitigate security threats at minimal cost. Of the many possibilities, three prevalent architectures emerged.

The first focuses on directing data from edge devices (e.g., personal computer terminals, smartphones, etc.) to specific data centers through switches. The switches act as a spine to parse data based on type, amount and user. By encrypting the switch software, this switch strategy hopes to solve the issue of security and privacy. The second infrastructure focuses on filtering the data at the edge and only storing the data needed. The focus centers on the devices and sensors on the edge collecting data and the software sending wanted data once a pre-established threshold is reached. This strategy attempts to reduce data storage, bandwidth, and data latency through less throughput, thus reducing costs for businesses. The third cloud infrastructure packages services based on need. Users can decide to purchase storage space or the device itself, the service and/or the software to run it or allow the firm to do so. This strategy tries to provide the consumer the software, platform and infrastructure to run it. Of course, not many firms within the industry have the capacity and capability to do so.

The fundamental issue with the cloud infrastructure is the trade-off between the cost of owning and operating servers and data centers and maintaining the privacy and security of the data. Ultimately, organizations will determine the best cloud infrastructure based on specific business strategies and market conditions. Large businesses may decide to keep their data centers 'localized' where they can control and secure the data themselves, but will incur an added infrastructure cost. Smaller businesses, on the other hand, may opt to use a cloud solution to store their data to reduce costs while ensuring adequate security. In either case, the cost of high performance computing and storage continues to drop. The large long term costs originate with the electrical and cooling costs associated with physically maintaining the computing devices. The cloud infrastructure outlook will most likely take on a hybrid approach dependent upon the business using the cloud. This suggests that the cloud infrastructure can and should have enough differentiation to accommodate all forms of businesses vice any single system becoming dominant.

Mobile Technology -- A Game Changer

The International Telecommunications Union (ITU) reports that 3 billion people, 40 percent of the world's population, have access to the Internet.[105] By 2025, there will be at least two billion more users[106], many of whom will access the Internet solely via mobile devices. Consumers are gravitating towards mobile devices as their primary means to access the Internet rather than through the desktop or personal computer. In 2014, global mobile traffic grew by 69 percent and is expected to increase ten-fold by 2019 with the Middle East and Africa projecting the strongest growth.[107] More than half of the world's population that owns a cell phone will use mobile technology to access the Internet to consume and share information, conduct e-commerce, and access social media. The impact of the mobile technology explosion has resultant benefits to industry and the global economy, especially as the smartphone becomes more capable and more affordable.

A study conducted by Business Insider reports that Americans spend more time on social media than any other major Internet activity, including email, thereby creating economic value in a previously non-existent market.[108] Social media giants have capitalized on the consumer's shift to mobile devices. Sources from two large social media firms indicated that transitioning from a desktop platform to a mobile platform is a key strategic initiative. Both have seen an increase in monthly active users and significant revenue from advertising generated from mobile devices. As

social media platforms expand in functionality, they are becoming a behemoth for big data collection and the entry point for e-commerce transactions.

Internationally, increasing numbers of people are connecting to the Internet via mobile technology as wireless infrastructure reaches undeveloped areas. As in the US, mobile carriers have partnered with social media giants to pre-populate mobile phones and tablets with popular social media applications. It is important to note that non-democratic countries often block popular Western social media sites to limit Western influence. As such, they generally have their own social media platforms that serve as a good medium for communication, networking, and e-commerce, limiting market access by 'foreign' advertisers to consumers in these non-democratic countries. The international community must determine if this violates any "equal access" provisions within trade agreements.

Internet of Things (IOT) -- Trend of the Future

Advances in cloud computing and big data analytics along with the huge increase of mobile devices has laid the groundwork for an explosion of smart, connected devices called the Internet of Things (IOT). Consumers are demanding more mobile devices, wearables and smart, connected devices like thermostats and cars. Smaller sensors and processors along with better software, encryption algorithms, and analytics engines will continue to drive this trend long term (5-15 years). This technology will diffuse into other industries (automotive, transportation, food services, etc.) allowing firms to increase productivity by displacing less efficient and less effective manual intervention. It will also allow firms to collect data and analyze market behavior to predict needs and meet demand for innovative products and services. Roughly 10 percent of the economic value generated by the Internet of Things (IOT) is created by the "things", while 90 percent comes from connecting these "things" to the Internet.[109] IOT is the future of the industry, but the trade-off between connectedness and privacy/security will determine the pace at which this trend grows.

ICT and National Security -- The Overarching Concern

Another challenge the US ICT industry faces is the potential balkanization of the Internet by non-democratic countries who, by their sheer size, can redefine the global standards for ICT devices, wireless communications, content, and access. This presents an economic national security concern if the US loses that advantage. The US could see reduced GDP if non-market, non-democratic societies are able to overpower the market with their ICT products. The challenge to US firms is three-fold. First, due to ideological and political differences, non-democratic countries already produce their own mobile devices preloaded with software that limit market access to international producers (and to their own consumers). Second, producers in these countries often receive a market advantage due to regulatory fiat, something that is far less prevalent in more competitive OECD country markets. Third, due to low labor costs, the countries are able to manufacture cheaper mobile devices that are attractive to lower-income countries.

An estimated 2 billion more people will come online in the next 10 years,[110] most of them in the developing world and most of them using mobile devices. As this happens, firms from these non-democratic countries may be able to leverage these advantages to increase their market power. Consequently, the US may find only limited opportunities in the global ICT market or discover they must change their practices to meet the new foreign standards. The non-democratic countries also may be able to exploit globally-generated economies of scale to compete with US firms in the US. To counter this shift, the US ICT industry and US government trade officials must work with trade restricted countries and negotiate a presence in their markets. This shift will be gradual

because transportation and shipping costs are an issue and because developing countries are only slowly building their middle class who can afford to purchase these products.

Finally, a potential problem gripping the US ICT industry today, in our considered opinion, is they do not adequately focus on lesser developed and non-democratic foreign markets. The general sense, we observed, from visiting Silicon Valley is "Why bother? There is enough of a market here in the US." True to their point, many US ICT firms are successful, as measured in billions in revenues, without focusing on these emerging markets. But how long can it last? Will the domestic market and mature foreign markets eventually saturate? To curb this economic national security concern, the US ICT industry may need to focus more internationally, realizing that the US could lose its economic advantage. A promising trend is the focus by Google and Facebook on spreading Internet connectivity to underserved regions and countries using air and space platforms. Perhaps this signals that the ICT industry is starting to focus on the potential market in the developing world. The other advantage the US has is its soft power to attract the rest of the world with respect to information availability and sharing. E-commerce or other consumer-focused ICT applications are relatively easy to spread worldwide, so US competitors with enough economy of scale could become the market leader. However, these same competitors may not have the soft power to attract the rest of the world with respect to information availability and sharing the way the US does. The US should capitalize on this distinct advantage to further its vision of a free and open Internet and lessen the economic effect on our national security.

GOVERNMENT'S ROLE

The role of the US Government with regard to the ICT industry is to create an environment that facilitates and enhances the competitive characteristics of markets and to mitigate the effects of market failures, especially those that are state-induced. Good governance practices spur innovation and competition, ultimately leading to enhanced productivity, economic growth, and national security. This section provides recommendations to address the challenges and issues that have been raised throughout this report.

Technological Advantage

The following recommendations enable the government to stimulate R&D without incurring radically diminishing returns to the point of waste, while considering the still-sluggish economy and a government dealing with sequestration.

- Increase and make the R&D tax credit permanent so that corporations can include it in their strategic planning.
- Shift to "Territorial" tax treatment for overseas profits which encourages repatriation of cash and further investment in the US.
- Incentivize federal and private research labs to collaborate and create research consortiums to tackle our wicked problems. These public/private partnerships will leverage best-of-breed concepts from each to create game-changing innovations.
- The federal government should increase R&D funding for the Networking and Information Technology Research Development (NITRD) to ensure that it keeps pace in IT innovation with the rest of the world.

- Congress should pass the Research and Development Efficiency Act, which establishes a working group to review federal regulations to eliminate redundancies and reduce regulator burden on universities.[111]
- Create innovation clusters where scientists and engineers can closely collaborate resulting in tremendous innovation and growth.[112]

Human Capital

Educated and trained human capital is crucial to the future health of the ICT industry. Recognizing that the federal government has limited authority vis-à-vis education and that the lack of STEM personnel may be attributable more to problems with primary and secondary education than with tertiary education, the following recommendations are general in nature. They offer ideas of creative ways to encourage students to pursue STEM education.

- Have the status of critical human capital skills briefed at regularly scheduled meetings of the National Security Council (NSC). This group must include representatives from at least the Department of Labor, Department of Commerce, Department of Treasury, Department of Education, and the Department of Defense. This report will be used at the NSC to direct the strategy for maintaining sufficient human capital in strategically critical industries. The intent is to ensure that this issue is being given the strategic attention that it warrants.
- Develop a system or process to identify the human capital differential between the supply from the nation's educational institutions and the demands of critical industries.
- Consolidate the 209 different STEM programs in the federal government into a single agency that has NSC approved strategic objectives to accomplish. This consolidation must be supported with clear strategic objectives to shape a cohesive set of programs for education.
- Following the lead of states that are approving "differential tuition" for students selecting a STEM major,[113] the Department of Education should make this a federal program and apply it to all federally- and state-funded schools across the nation.
- To increase the number of teachers with STEM degrees, provide education grants to undergraduate students who commit to a STEM degree. These students would be required to teach in a STEM-related field for at least five years. (Note: this is similar in concept to the DoD's Reserve Officer Training Corps program.)

The following recommendations address the gap between ICT job openings and qualified candidates. This is a short- to mid-term solution while STEM education initiatives are given time to increase the number of qualified job applicants.

- Modify the H1-B visa system so it can fill the human capital gaps in critical industries. This could include removing arbitrary caps on the number of H1-B visas, providing the flexibility for an increased number of visas or a longer visa duration based on annual supply shortfall and industry demand.
- As part of immigration reform, ensure considerations are made to attract and retain highly skilled immigrants to work in the US. This promises to fill the human capital gap, bolster our knowledge capital and innovation, and keep the workforce young and motivated.

Security

The following recommendations enable the US to maintain an open and reliable Internet while ensuring privacy and national security.

- Establish cooperative research agreements and establish consortiums to leverage expertise in the government with that of private industry to develop the best of breed encryption technologies such as quantum encryption (e.g. leverage the Defense Advanced Research Projects Agency and team it with industry on this initiative).
- Invest in next generation intrusion detection systems that use artificial intelligence.
- Develop technologies such as built-in-chip defenses and "Zero Day" countermeasures to counter microprocessor manufacturing concerns.
- Improve supply chain assurance through an AS-9100-like quality standard, an expanded Trusted Foundry Program (NSA) and planting Foundries in friendly low cost nations through FMS offset programs and private incentives.
- Adequately resource DHS in their capacity as the designated lead for federal government cybersecurity to lead the establishment of a domestic cybersecurity framework.
- Clarify boundaries between public and private sector cybersecurity responsibilities.
- Resource critical infrastructure upgrades (e.g. Smart Grid) to enhance security.
- Continue to Update FISMA/Title 44 to enable a modern approach to federal cybersecurity and ensure adequate resourcing.

Governance

The following recommendations will improve governance vis-à-vis the ICT industry.

- Congress should pass cybersecurity information sharing legislation that will provide liability coverage for the private sector and encourage information sharing between private corporations and between private and public segments to improve infrastructure security (safeguards would also need to be in place to prevent collusion).
- Federal agencies should immediately begin implementation of the Federal Information Technology and Acquisition Reform Act (FITARA), empowering CIOs to drive agency investment and implementation.[114]
- DoD should undertake a study to determine the best acquisition model for offensive and defensive cyber systems. Due to the dynamic nature of the cyber threat and the nature of offensive cyber tools, a traditional acquisition model may not be agile enough. Options could include designating USCYBERCOM to be the Milestone Decision Authority or adopting a quick reaction capability (QRC) model as the standard model for offensive cyber tools.
- The US should pursue a *light-touch* regulatory framework for broadband. This will continue US investment and innovation that has created the most capable network and most innovative content in the world.[115] In light of the recent FCC Open Internet Order, the best option is for Congress to pass legislation institutionalizing the *light-touch* framework while still protecting Net Neutrality principles.

CONCLUSION

The outlook for the ICT industry is highly positive based on the strength of its firms, the quality of its people, and significant future market opportunities. The software, IT services, and wireless segments are performing well and growing while the manufacturing and wired segments are stressed and experiencing shrinking revenues. In all segments, firms rely upon innovative products and services to compete against domestic and foreign competitors and must therefore invest heavily in R&D. This need for innovation also creates a demand for highly-skilled human capital. To maintain the US edge in innovation, the government should act to stimulate R&D spending and to address the human capital shortfall in STEM-educated workers.

The ICT industry has provided enormous stimulus to the US economy. It does so directly through sales of products and services and indirectly by facilitating productivity gains in other industries. This trend will continue as mobility, cloud computing, and the Internet of Things offer new productivity gains to other industries. These prospective gains are only possible if companies continue to innovate and invest in broadband and related ICT infrastructure. To facilitate this, the government should take a *light-touch* approach to regulation and legislation, only intervening to address market failures. This *light-touch* approach has enabled the past 30 years of extraordinary progress and should be continued.

As ICT products and services proliferate and the world becomes more connected, the cyber threat increases. This is one of the most significant challenges facing the industry today. Overcoming this challenge will require a coordinated response by government and industry. The government must provide a legal framework and resources to protect critical infrastructure and government systems and must facilitate information sharing with industry. Both government and industry must invest in new cybersecurity technologies to address the growing threat.

If the US can overcome these challenges, the ICT industry should be well-positioned to remain the global ICT leader. It will stand ready to capitalize on the latest ICT trends--mobility, cloud computing and the Internet of Things--and it will be the leader in charting new trends. This offers significant economic potential, which ultimately ensures US national security.

Appendix A
In-Class Visits

Speakers representing:

Federal Communications Commission
FirstNET (The First Responder Network Authority)
J-Capital Research (on China's economy)
Microsoft
National Security Agency
National Telecommunications and Information Administration
Joint Staff J-6
New Atlantic Ventures (a technology-focused venture capital firm)
Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
The Defense Industrial Base
US Patent and Trademark Office

Appendix B

Strategic Financial Analysis

(data from Morningstar.com)

Table 2. Industry Analysis for Communication Manufacturing, NAICS 33422

	HRS	CSCO	ALU						
Market Share from this Industry	8.7%	14.7%	12.1%						
Revenues from this Industry ($Mil)	$ 3,002	$ 5,072	$ 4,175						
Co Total Revenues	$ 5,012	$ 47,142	$ 19,100						
% of Co's total Revs from this Industry	59.9%	10.8%	21.9%						
	Last 5 yrs average					5y Trend (CAGR)			
Profitability (as % Revs)	HRS	CSCO	ALU	Ave for Big 3		HRS	CSCO	ALU	Ave for Big 3
Gross Margin	34.3%	58.5%	33.2%	42.0%		-5.6%	-8.6%	-0.89%	-5.0%
Net Income	6.8%	17.2%	-4.1%	6.6%		-9.2%	-1.1%	-10.0%	-6.7%
Capex	4.4%	2.6%	3.6%	3.5%		-32.3%	-0.7%	-17.5%	-16.8%
R&D	not rptd	12.8%	16.5%	14.7%			-3.4%	-1.4%	-2.4%
Financial Performance									
ROA	7.0%	8.6%	-6.1%	3.2%		-8.4%	-22.0%	0.0%	-10.1%
ROIC	11.9%	12.1%	-2.30%	7.2%		9.2%	-6.1%	-121.07%	-39.3%
Financial Health									
Current	1.7	3.3	1.4	2.1					
Quick	0.9	3.0	0.9	1.6					
Financial Leverage	2.8	1.8	7.6	4.1					
Debt/Equity	0.9	0.3	1.5	0.9					
Interest Coverage	9.0	17.6	-2.1	8.2					

Table 3. Industry Analysis for Wireless Telecommunications, NAICS 51721

Wireless - 51721											
Verizon, AT&T, Sprint, T-Mobile	VZ	AT&T	S	TMUS							
Market Share from this Industry	39.3%	32.4%	6.9%	12.2%							
Revenues from this Industry ($242,100M)	$ 95,145	$ 78,440	$ 16,891	$ 29,564							
Co Total Revenues	$ 127,079	$ 132,447	$ 16,891	$ 29,564							
% of Co's total Revs from this Industry	74.9%	59.2%	100.0%	100.0%							
	Last 5 yrs average						5y Trend (CAGR)				
Profitability (as % Revs)	VER	AT&T	S	TMUS	Ave for Big 4		VER	AT&T	S	TMUS	Ave for Big 4
Gross Margin	60.00%	56.00%	44.0%	45.0%	53.3%		3.60%	-6.40%	-14.3%	11.4%	-1.4%
Net Income	5.17%	8.00%	-10.0%	1.5%	1.1%		21.39%	13.07%	-23.6%	28.0%	9.7%
Capex	15.00%	16.00%	14.0%	20.0%	15.0%		-10.60%	-1.00%	79.9%	28.8%	24.3%
Financial Performance											
ROA	2.47%	3.75%	-5.0%	2.0%	0.4%		15.20%	-57.60%	-37.1%	-81.8%	-40.3%
ROIC	7.91%	7.49%	-5.0%	5.0%	3.5%		16.40%	-59.20%	-39.7%	-45.9%	-32.1%
Financial Health											
Current	1.06	0.86	0.85	1.59	0.9						
Quick	0.90	0.62	0.66	1.18	0.7						
Financial Leverage	18.92	0.03	3.76	3.62	7.6						
Debt/Equity	8.99	0.88	1.41	1.56	3.8						
Interest Coverage	4.11	3.76	-0.98	1.31	2.3						

Table 4. Industry Analysis for Software Publishing, NAICS 51121

	MSFT	ORCL	IBM						
Market Share from this Industry	19.5%	6.8%	4.2%						
Revenues from this Industry ($Mil)	$ 38,240	$ 13,335	$ 8,236						
Co Total Revenues	$ 86,833	$ 38,275	$ 92,793						
% of Co's total Revs from this Industry	44.0%	34.8%	8.9%						
	Last 5 yrs average					5y Trend (CAGR)			
Profitability (as % Revs)	MSFT	ORCL	IBM	Ave for Big 3		MSFT	ORCL	IBM	Ave for Big 3
Gross Margin	73.83%	79.43%	48.70%	67.32%		1.20%	3.06%	8.46%	4.24%
Net Income	26.60%	26.83%	14.69%	22.71%		10.20%	-9.50%	12.70%	4.47%
Capex	4.52%	1.60%	4.41%	3.51%		168.00%	20.60%	7.64%	65.41%
R&D	13.20%	12.90%	6.00%	10.70%		0.00%	15.42%	-2.82%	4.20%
Financial Performance									
ROA	17.40%	3.70%	12.78%	11.29%		-44.97%	3.10%	-26.03%	-22.64%
ROIC	27.80%	17.45%	27%	24.18%		-52.10%	5.07%	-28.44%	-25.16%
Financial Health									
Current	2.50	2.92	1.53	2.32					
Quick	2.29	2.69	1.46	2.15					
Financial Leverage	1.87	1.91	10.35	4.71					
Debt/Equity	0.18	0.43	5.30	1.97					
Interest Coverage	79.00	15.56	47.00	47.19					

Table 5. Industry Analysis for IT Consulting, NAICS 54151

	IBM	HPQ	EMC	ACN							
Market Share from this Industry	6.2%	4.1%	1.5%	1.5%							
Revenues from this Industry ($Mil) (354,200 total)	$21,960	$14,522	$5,313	$5,313							
Co Total Revenues	$92,793	$110,139	$24,440	$32,418							
% of Co's total Revs from this Industry	23.7%	13.2%	21.7%	16.4%							
	Last 5 yrs average						5y Trend (CAGR)				
Profitability (as % Revs)	IBM	HPQ	EMC	ACN	Ave for Big 4		IBM	HP	EMC	ACN	Ave for Big 4
Gross Margin	48.70%	23.52%	62.15%	30.45%	41.21%		6.70%	2.90%	2.60%	-1.70%	2.63%
Net Income	14.69%	4.76%	11.80%	9.30%	10.14%		-19.00%	-43.50%	42.80%	69.60%	12.48%
Capex	4.41%	3.28%	6.03%	1.19%	3.73%		3.20%	-3.10%	-2.10%	-31.80%	-8.45%
R&D	6.00%	2.88%	11.78%	0.00%	5.17%		0.20%	22.70%	14.00%	0.00%	9.23%
Financial Performance											
ROA	12.78%	5.55%	6.55%	15.91%	10.20%		-21.80%	-31.00%	-4.00%	18.20%	-9.65%
ROIC	27.30%	11.67%	11.24%	63.42%	28.41%		-31.30%	-5.60%	-20.90%	-14.90%	-18.18%
Financial Health											
Current	1.53	1.10	1.29	1.47	1.35						
Quick	1.46	0.71	1.05	1.25	1.12						
Financial Leverage	10.35	3.95	1.95	3.57	4.96						
Debt/Equity	5.30	0.67	0.19	0.01	1.54						
Interest Coverage	47.00	21.64	29.65	262.82	90.28						

Appendix C
Corporate Income Tax Effects

Large US multi-national ICT corporations such as IBM, Microsoft, Oracle, and Apple obtain a significant portion of revenue and profit overseas. US tax regulations have a large negative impact on private investment within the ICT industry. At 39 percent, US tax rates are much higher than all other developed nations, causing avoidance of taxes by maintaining large amounts of capital overseas vice in the US financial markets.

According to Mintz and Chen, compared with a *territorial* tax system which taxes profits only in countries where they are earned, America's *worldwide* tax system has not kept pace with a competitive global environment. "Since 2005, 63 of 95 countries surveyed have cut their [OECD] average statutory tax rates to 24.4 percent, while the US has remained stagnant at above 39 percent."[116] According to KPMG, by 2014 the US had the highest corporate tax rate among Prominent Developed Countries—even higher than Japan (36 percent) and France (33 percent).[117]

It should be no surprise that companies are relocating to lower-tax domiciles. In 2000, 17 percent of non-US OECD Forbes 500 companies were headquartered in countries with a territorial tax system. By 2012, that figure had grown fivefold to 90 percent.[118] While more research needs to be done to determine how much ICT business has moved out of the US due to tax policy, it is clear than ICT companies already doing business overseas are avoiding repatriating those profits to avoid high US Taxes. Companies are using creative strategies such as "inversions" to improve profitability. According to Gabriel Zucman, "US corporations book 20 percent of their profits in tax havens, a tenfold increase since the 1980's; their effective tax rate has declined from 30 to 20 percent over the last 15 years, and about two-thirds of this decline can be attributed to increased international tax avoidance."[119] More than $2 trillion in US-based company profit may be "locked-out" from both US taxation and reinvestment.[120] Cisco Systems alone reported that in 2013 its taxes were $1.8 billion less than they would have been if all of its earnings had been taxed at US rates.[121] Companies can use their overseas cash without repatriation by investing it in the domiciled country, by making a foreign company acquisition, or borrowing the amount of "locked-out" proceeds and using the cash for dividend payments, or share repurchases. Despite being incredibly solvent in mid-2014, instead of repatriating $17 billion, Apple borrowed the money and paid a portion to its shareholders. It made more financial sense to pay a few points of interest on that debt than to pay $4.4 billion in taxes at their 26.2 percent effective tax rate.[122] The table below shows that many other American ICT companies make extensive use of havens to avoid repatriation taxation.

2013 Untaxed Foreign Profit of Large ICT Companies[123]

Company	Untaxed Foreign Profit ($B)	Company	Untaxed Foreign Profit ($B)
Microsoft	76.4	Oracle	39.3
Apple	54.4	Google	38.9
IBM	52.3	Hewlett-Packard	38.2
Cisco	48.0	Intel	20.0

Source: "Repatriating Games" *Shareowner* (Online) 29 (1): 4-5.

We know that companies do respond to tax policy changes. For example, Engel and Lyons report that, "As part of the American Jobs Creation Act of 2004, companies were allowed to repatriate overseas cash at a reduced rate of 5.25 percent. The Internal Revenue Service (IRS) reported that 843 companies took advantage of this and that $312 billion was repatriated. That resulted in a tax savings of $265 billion for the companies."[124] Addressing only the eight companies in the table above (assuming a competitive US tax policy revised to equal the OECD effective rate of 24.4 percent), the US would capture $89 billion in tax revenues.

R&D Tax Credit Effects

The Innovation and Technology Foundation reports that every US federal dollar spent R&D tax credits spurs $1 to $2 of business R&D investment.[125] A 2012 study of French firms by Duguet found that one Euro of tax credit yields slightly more than one Euro of total R&D, while also increasing the number of R&D researchers.[126]

Conclusions

US Tax Policies are creating incentives for many multinational corporations, including American ICT companies, to stash *trillions* of dollars overseas, "locked-out" from US taxation. Creative tax-haven strategies like borrowing to pay dividends and conduct share buybacks to deliver some returns to shareholders. However, some of the full benefit is likely lost through unnecessary transaction costs, and opportunity cost losses from foregoing more financially efficient US investments in favor of keeping the money overseas. For small to medium sized businesses (SMB), R&D tax credits stimulate at least an equivalent amount of new R&D investment. Many tech breakthroughs occur at SMB level and generally reach the broader market when their technologies are transferred to larger firms through licensing or M&A activity. However, by definition, R&D is a long term proposition. Accordingly, R&D tax credit policy needs to be dependably stable over long periods of time, or many companies will decrease their R&D investments to compensate for the uncertainty of receiving offsetting future tax credits.

Appendix D
Resourcing Trusted Microprocessor Supply

Overview

The US' rising dependence on imports of microprocessors (MPs) manufactured in China represents a substantial threat to national security. As the world rapidly becomes more digitally-interconnected through the explosion of mobile devices and the emerging "Internet of Things" (IOT), nearly every device, vehicle or platform powered by electricity will contain digital microprocessors. In addition to our military's reliance on electronics as the brains of our modern weapon systems, the US Government spends more than "$81 billion annually for information technology (IT) systems, components, software, and related services, and it is highly reliant on IT to perform its many functions and responsibilities."[127] Media coverage of recent hacking attacks on large companies such as *Sony Pictures Entertainment* and *Target Corporation* have piqued the public's awareness regarding the country's vulnerability to internet-based hacking attacks. As a result, both the White House and Congress have begun to pay some attention to internet-based threats and network security vulnerabilities. However, due to massive complexities in the supply chain and the impracticality of testing every purchased component, compromised MP hardware may represent an even larger threat that is more challenging to detect and more difficult to counter than any internet-based threat. Issue number 11 in the White House's *Comprehensive National Security Initiative* (CNCI) highlights the need for action:[128]

> **Initiative #11. Develop a multi-pronged approach for global supply chain risk management.** Globalization of the commercial information and communications technology marketplace provides increased opportunities for those intent on harming the US by penetrating the supply chain to gain unauthorized access to data, alter data, or interrupt communications. Risks stemming from both the domestic and globalized supply chain must be managed in a strategic and comprehensive way over the entire lifecycle of products, systems and services. Managing this risk will require a greater awareness of the threats, vulnerabilities, and consequences associated with acquisition decisions; the development and employment of tools and resources to technically and operationally mitigate risk across the lifecycle of products (from design through retirement); the development of new acquisition policies and practices that reflect the complex global marketplace; and partnership with industry to develop and adopt supply chain and risk management standards and best practices. This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks.

In addition to underlining the nature of the MP-based threat and proposing general strategies to reduce global supply chain vulnerabilities, this paper specifically addresses the China-based problem. Doing so requires the reader to understand MP-related economic trends, how the Chinese MP manufacturing industry competes given these trends, and its strategic vulnerabilities.

Economic Trends and China's Strategy in the MP Value Chain

A combination of the explosion in demand for distributed applications and mobile computing, the "internet of things", and Moore's Law fuels demand for smaller, more powerful MPs. For example, a typical 1990's luxury car contained 3-10 MPs. Today that same model car might be dependent upon 100 MPs and 100 million lines of code. This order of magnitude increase requires more than 5000 new designs annually.[129] In the 1980s, building a MP fabrication manufacturing facility cost $200 million (2014 $USD) *(Fig1).* American companies relied on very few subcontractors, performed nearly all the steps in the value chain, and maintained sole accountability for quality assurance and security of their products. Today, building a modern MP manufacturing plant or "foundry" costs $7 billion, and some experts predict it may cost $20 billion by 2020.[130] In combination with demand for highly specialized designs, such massive entry barriers force firms into specialization. As a result, hundreds of suppliers compete at each value chain step, making it

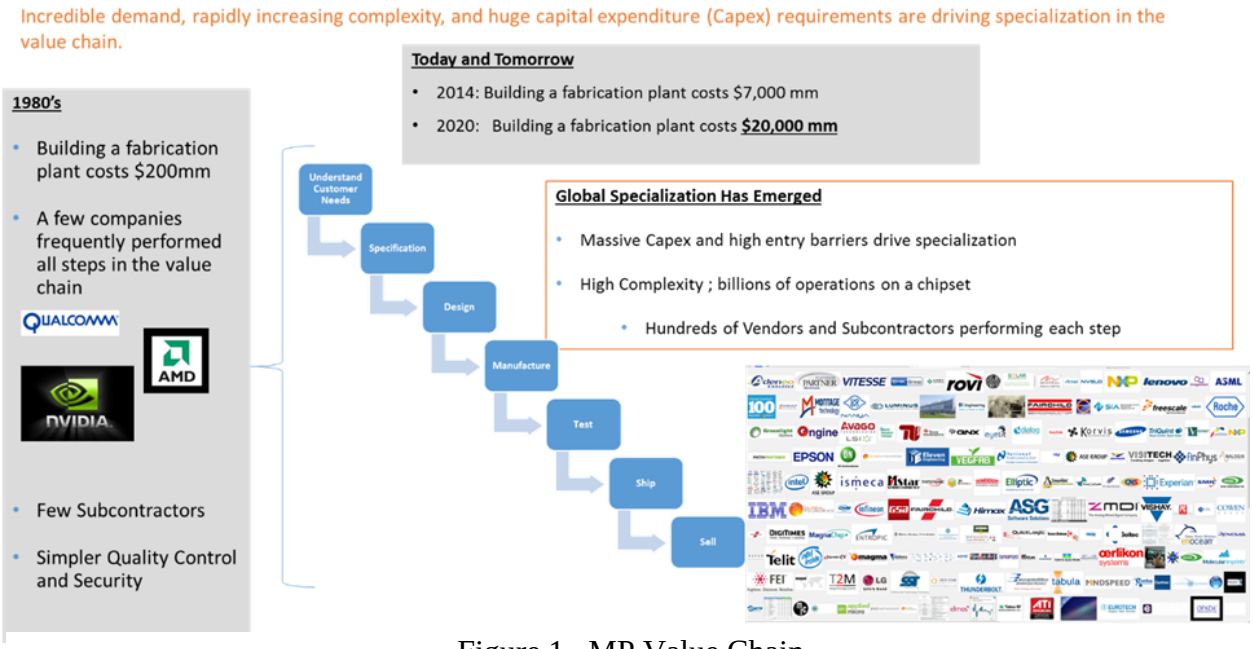

Figure 1. MP Value Chain

nearly impossible for system integrators to keep track of component sources.

Spotting the emerging trends and opportunities to leverage their low labor costs and available capital, the Chinese government made massive investments in MP manufacturing over the past two decades. Having entered the market first in manufacturing, Chinese firms have relied on their government's help to keep MP labor costs low (only 2 percent of revenues)[131] and subsequently have moved up-market into the design and specification elements in the value chain *(Fig 2).*

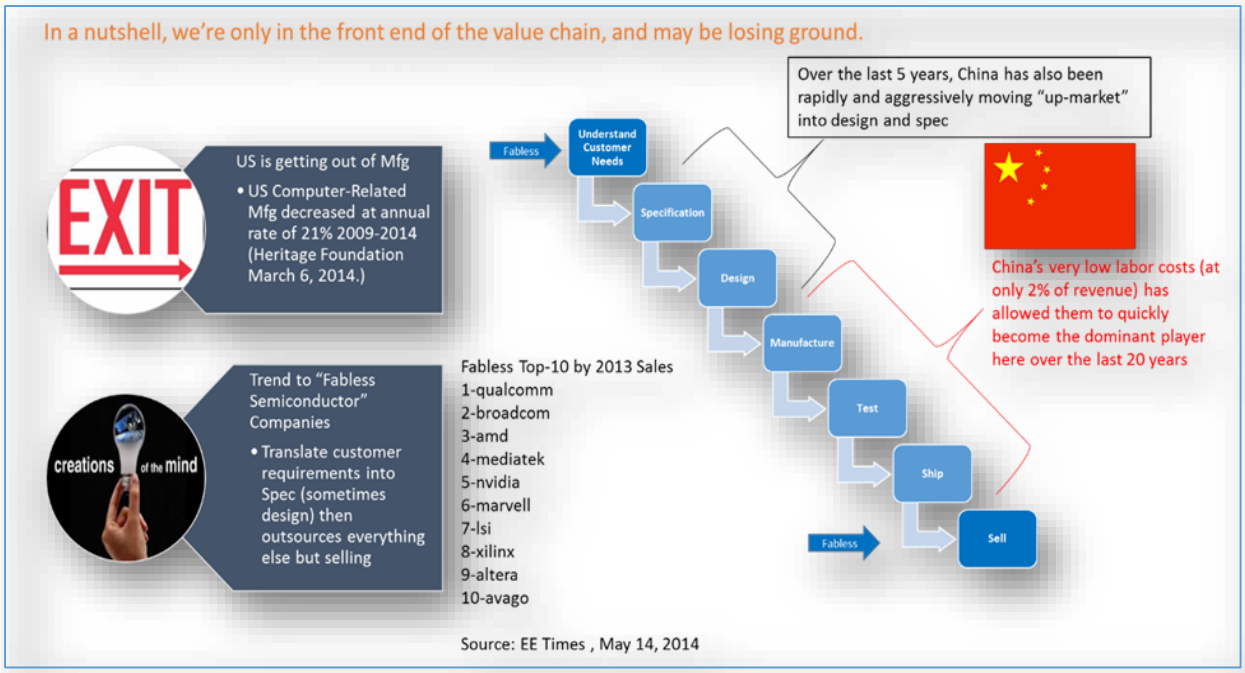

Figure 2. American Value Chain Trends

China is now both the largest consumer and largest exporter of MPs *(Fig 3)*, fifty-two percent of its production is exported, and it has doubled its share of the world market in the last decade (*Fig 4)*.[132]

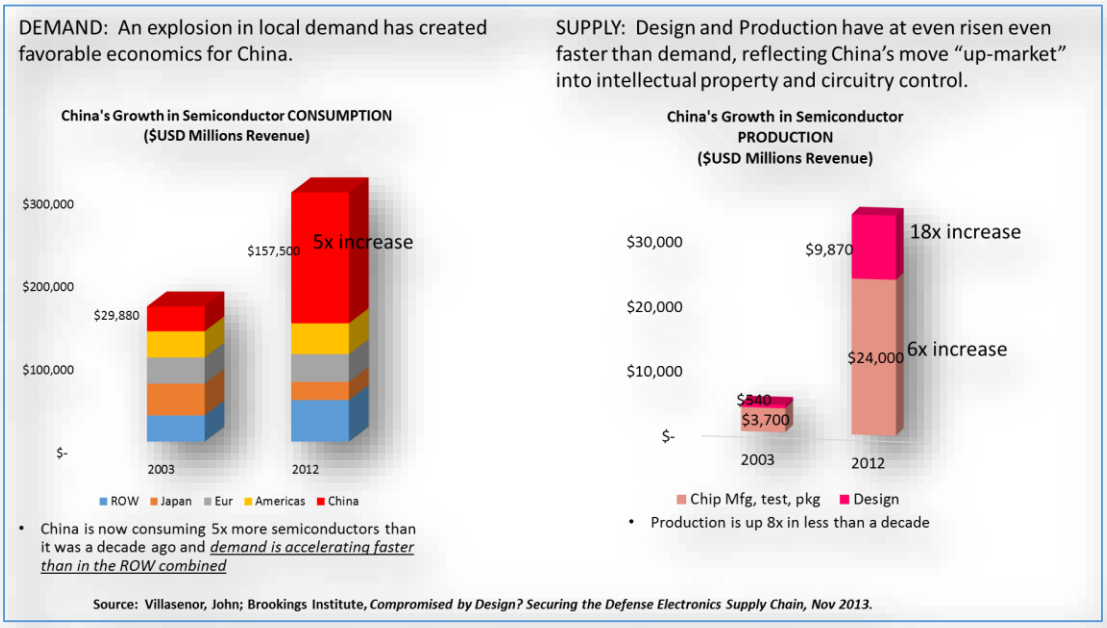

Figure 3. China's Demand and Supply Explosion.

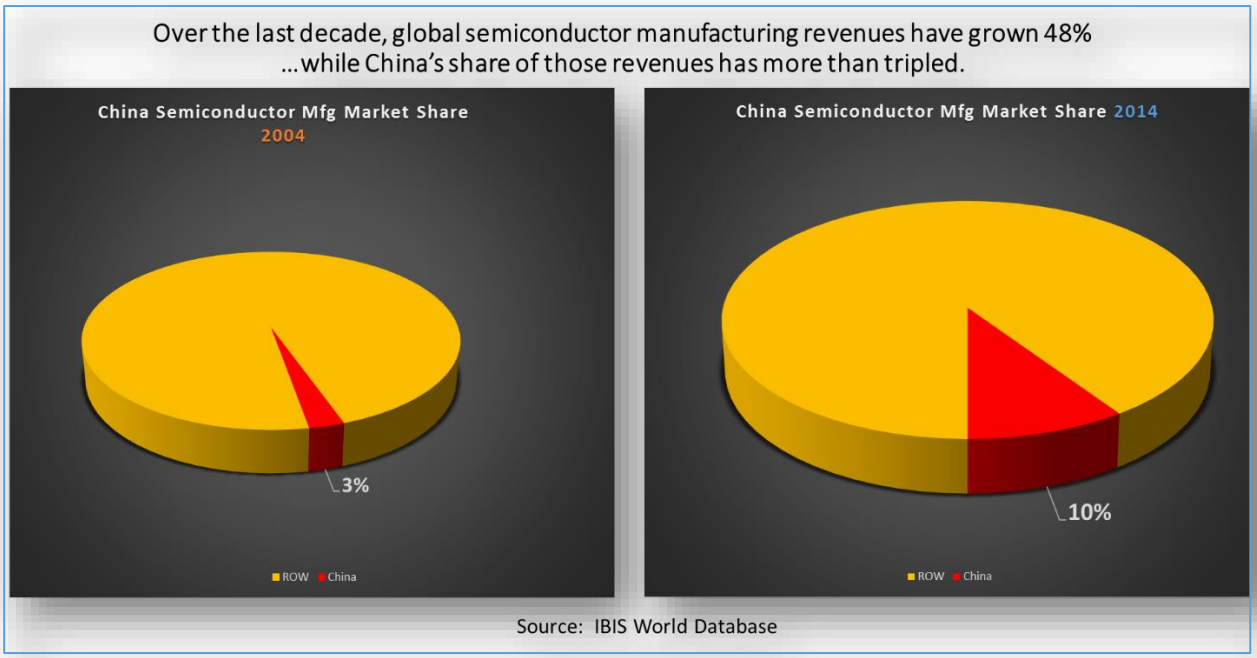

Figure 4. China's Rapidly Growing Global Market Share

China's financial support from its government and labor cost advantages have driven US firms out of nearly every step in the chain except for design and selling, where intellectual property and customer relationships remain critical to success. In fact, US firms are exiting the entire computer manufacturing sector at an alarming annual rate: 21% from 2009-2014.[133] America's rising dependence upon China subjects us not only to hold-up risk, but also to threats embedded in MP silicon and on-chip firmware.

The MP Problem: A Different Kind Of Cyber Threat

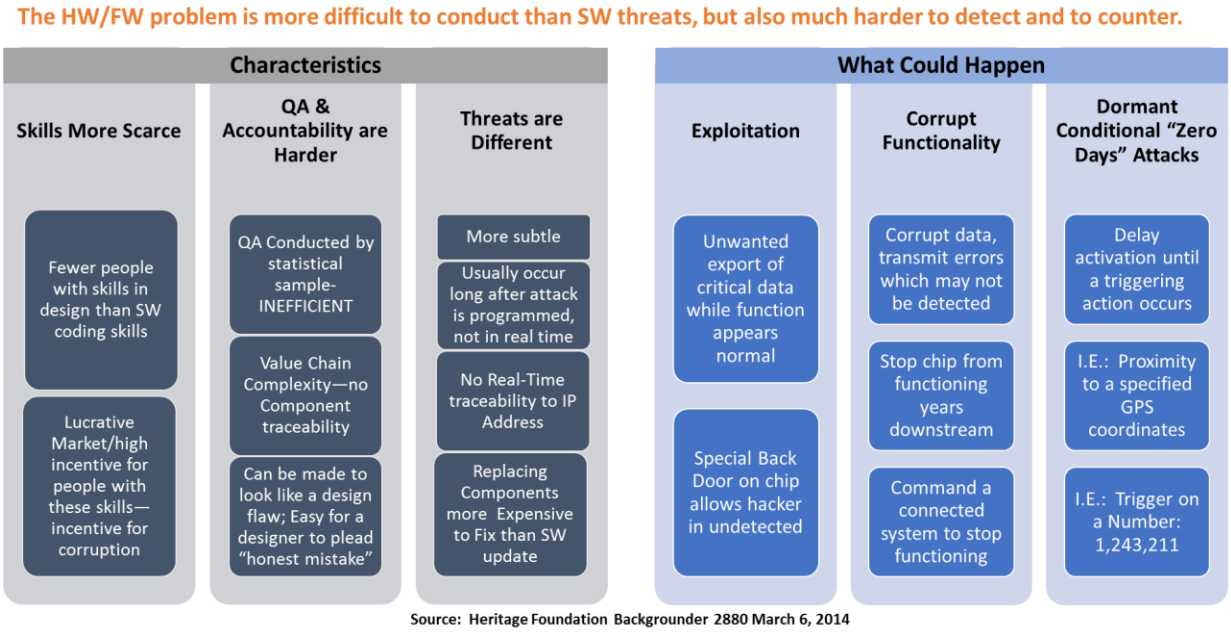

Figure 5. Why the MP Threat is Different and What Could Happen.

See Figure 5. Since control logic and firmware are burned into a MP during manufacturing, detecting and thwarting potential attacks may prove to be a greater challenge than it is with other cyber threats. Unlike malware embedded in software or attached to an email, execution of an attack is not easily linked to an associated event such as launching a program or opening a file. And, unlike an external hacker attack on a network, which may be traced to its source IP address, without meticulous documentation of personal accountability for each step in the value chain, MP attack sources would remain untraceable. The only way to prevent these threats would be to test every MP before employing it in a system—a costly, time consuming, and impractical solution with currently-available test capabilities. Corrupt MPs might covertly capture data and export it to another source while appearing to function normally. A pre-programmed "special back door" could allow a hacker into a system undetected. An MP could intentionally introduce undetectable computational errors into a critical system such as an aircraft's "fly by wire" controls, or perhaps command a connected system to stop functioning. Easily disguised to look like an unrelated system failure, such malware would prove difficult to trace to the perpetrator. Additionally, "Zero Days" attacks would delay activation until years after the MP's installation, and made to look like a routine malfunction. Moreover, *conditional* attacks, such as launching malicious functionality concurrent with the host system's proximity to certain GPS coordinates, could wreak havoc on military systems. Finally, even if the offending MP could be isolated, it might be nearly impossible to trace the malware origin back to the design engineer who programmed it; even if confronted, he could claim he made an unintentional error.

Analysis of Chinese Strategy, and the Approach to Counter It

Figure 6 depicts China's MP manufacturing strategy and its vulnerabilities. China makes huge capital bets to build foundries, then exploits very low labor costs and manipulation of its currency to bolster exports. However, rising costs and competitive pressures have squeezed profit margins down more than 60% in 8 yrs. China's reliance on this strategy renders it vulnerable to factors shown in the black box in Fig 6. Bringing about these conditions becomes the basis of our strategy.

Figure 6. China MP Manufacturing Advantages & Vulnerabilities. (Data Source: IBIS World China Database).

Ends, Ways, and Means

Applying an *Ascher-Overholt* model, the author analyzed *Ends*, *Ways, and Means* for *Core*, *Basic* and *Hedging* strategies (results are contained in Appendix A). *Table 1*, below, depicts a derivative analysis of those strategies: a prioritized table of *Capabilities (Means)* the US should implement applying a *Whole of Government* approach. It includes the lead agency, other key agencies with whom key coordination is required, and the projected time horizon for the first implementation. Items 9-15 are primarily *policy* issues and will not be addressed in this paper. Items 1-8 require significant resource commitments or substantial inter-agency coordination, and will be further amplified.

no.	Capability	Priority	Strategy Element	DIME Element	Lead Agency	Coordinate with	Horizon (yrs)
1	CyberAttack Defcon Posture with Disaster Response/Recovery	H	Core	M	DHS	DOD	3
2	Built-in Chip Defenses	H	Core	M	NSA	DARPA, DIB	3
3	Zero-Days Counter-Measures Stockpile	H	Core	M	NSA	DARPA, DIB	3
4	Alternative Intl Fabs through FMS Offsets	H	Core	E	DOD (FMS Offsets)	State, DIB	3
5	Trusted Foundry Program for hypercritical supplies	H	Core	M	DOD (OSD)	NSA	5
6	USG/Industry Cooperative Foundry Investments	H	Core	E	Commerce	State	5
7	Industry Process Standard (AS9100-like)	H	Core	I	Commerce	DIB	5
8	Quantum Computing	H	Core	M	DARPA	DOD	15
9	Promote China Culture	M	Basic	D	State	NGOs	10
10	Promote China Free Trade, Consumption and Middle Class Growth	M	Basic	E	Treasury	State, Commerce	10
11	Amicable, Stable Relations with neigbors and US	M	Basic	D	State	DOD	2
12	Counter-Terror Cooperation with China	M	Basic	I	DHS	DOD	2
13	Counter Currency Manipulation Tariffs/fines	L	Basic	E	Treasury	State	3
14	Economic Incentives/Premium Pricing for Compliance	L	Basic	E	Treasury	State	3
15	Insurance Bonding v. Cyber Attacks	L	Core	E	Commerce	DHS	5

Table 6: Prioritized Capabilities for MP Trusted Supply Assurance, Derived from Ascher-Overholt Analysis

Technologies

Table 2 contains an analytical summary of key technologies to be developed, leading and coordinating agencies, launch milestones, procurement horizons, funding sources, investment estimates, contract types and sustainment strategies. International partner possibilities, Iron Triangle issues, and Defense-Industrial Base issues, are also summarized. Each of these technologies addresses a different issue: *Defense*, *Offense*, and *Game-Changing*.

Capability	Built-in-Chip Defense R&D	Zero Days Countermeasures Stockpiles	Quantum Computing
Strategic Approach	DEFENSE	OFFENSE	GAME-CHANGING
Strategy Element	Core	Core	Core
DIME Element	M	M	M
Lead Agency	NSA	NSA	NSA
Coordinate with:	DARPA, DIB	DARPA, DIB	DARPA, DIB
Timeframe (yrs)	3	3	15
Funding Source	DOD (DARPA)	DOD (DARPA)	DOD (DARPA)
Estimate ($Millions)	$1000 (award 100x $10mm contracts)	$1000 (award 100x $10mm contracts)	$50 per year.
Launch Milestone	A	A	A
Contract Type	R&D	R&D	R&D
Development Stgy	Award 100 proposals for BICD technology demonstrators, looking for the most unique approach to defending against any threat. Then, LRIP produce MPs in trusted foundry the 10 most promising designs, and test in fielded systems.	Award 100 proposals for Software Designs. Conduct technology demonstrations. Select the best firms to be partners in continuous CM development.	Continuous funding of Basic Research to factilite breakthrough.
Sustainment Stgy	License slightly dumbed down versions to industry; deliver royalties to inventors. $100mm per year will be necessary to continously refresh R&D.	Select a limited number of firms to engage on a multiyear service contract to continously develop new offensive countermeasures.	Continuous funding of Basic Research to factilite breakthrough.
Allied Partners	Israel. UK.	Israel. UK.	Israel. NATO Nations.
Iron Triangle Issues	Justifying program will be difficult because tangible results will be hard to measure. Security and political sensitivities of technology co-development with UK and Israel must be managed by State and NSA. ITAR and Export Compliance may need special exceptions.	Justifying program will be difficult because tangible results will be hard to measure. Security and political sensitivities of technology co-development with UK and Israel must be managed by State and NSA. ITAR and Export Compliance may need special exceptions.	Politically difficult to explain. Invention could render all current encruption schemese obsolete. Possible international criticism that QC is being developed as an offensive cyber weapon. If breakthrough made by U.S., we may not want to share key technology with any other nation.
DIB Issues	Contracts may need to be spread amongst firms in all 50 states. Competitors will require security clearances.	Contracts may need to be spread amongst firms in all 50 states. Competitors will require security clearances.	Only a few research labs may be capable of running these programs.

Table 7. Key Technologies for Trusted MP Supply

Defensive Technology

The massive number of Chinese-produced MPs already in US systems suggests that we must assume that many of them are already compromised by time-triggered, or event-triggered zero-days maladies pre-programmed for future malevolence. Defending against already-compromised MP's embedded in US systems requires Built-In-Chip Defenses (BICDs). BICDs would monitor all connected MPs on a given platform, looking for a malfunction or malady. When one is detected, the BICD would isolate and bypass the malfunctioning MP, or even program itself to replicate the rogue MP's original functionality. A DARPA-NSA team cooperating with key international partners would manage procurement and security issues for up to one hundred $10

million contracts in pursuit of major breakthroughs. After down-selecting and testing the most promising designs, the program could be sustained by licensing slightly "dumbed-down" versions to industry, and using derived royalties to sustain further development activities. The nature of such an expensive program requiring segmentation, secrecy and limited oversight will make it difficult for Congress to support unless contracts are spread widely across contractors in many states.

Offensive Technology

Building our own stockpile of offensive *Zero-Days Countermeasures* (ZDCM) capabilities will equip the US with a deterrent to Chinese and other potentially malicious actors—enabling diplomatic *cyber détente*. Like BICDs, a DARPA-NSA team employing careful program and security compartmentalization and international cooperation would run a competition culminating in demonstrations and down-selects. The competition would generate an initial stable of offensive weapons. However, sustainment would then require continuous development of *Measures/Countermeasures*. Engaging the down-selected firms in a combination of fee for service research contracts to spawn follow-on product development programs over multiple years would sustain the competency. Also like BICD, spreading contracts across the US may need to be the inefficient compromise for obtaining Congressional support for a program that requires high levels of secrecy and restricted oversight.

Game-Changing Technology

Q*uantum Computing*'s (QC) theoretically massive computational capability might yield breakthroughs in MP *quality assurance.* Today's Non-Destructive Test (NDT) technologies have only limited applicability in MP circuitry testing. Most are too time-consuming, too function-specific, and too costly to test more than a very small random sample of MP inventories on a limited number of parameters. Combined with QC's ability to perform calculations billions of times faster than any other known computer, it's theoretically possible for a QC-enabled NDI system to simultaneously test every MP in an incoming inventory batch for complete hardware and firmware integrity quickly and cost-effectively. Moreover, in more advanced forms, QC's computational capability could quickly crack any known encryption key, or change an encryption algorithm instantaneously in the face of an active threat—both technologies that would revolutionize cyber defense and offensive cyber warfare.[134] Accordingly, the US needs to expand NSA's already-exiting QC program in cooperation with EU partners. QC is an early stage research activity that will likely take 15 years or longer to mature, even with significant steady funding of $50 million per year. Finally, as privacy issues become more of a concern in minds of US citizens, security professionals will need to work with the White House and Congress to effectively communicate the intentions and merits of the program so that they are not misunderstood.

Programs

Table 3 contains an analytical summary of key programs to be developed, leading and coordinating agencies, launch milestones, procurement timeframes, funding sources, investment estimates, contract types and sustainment strategies. International partner possibilities, Iron Triangle concerns, and Defense-Industrial Base issues are also summarized.

Capability	CyberAttack Defcon Posture with Disaster Response/Recovery	Expand Trusted Foundry Program for hypercritical supplies	Industry Process Supply Chain Standard (AS9100-like), and Ethical Standards	Offset-Funded Alternative Source international Foundries	USG/Industry Cooperative Foundry Investments
Strategy Element	Core	Core	Core	Core	Core
DIME Element	M	M	I	E	E
Lead Agency	DHS	DOD (OSD)	Commerce	DOD (FMS Offsets)	Commerce, Treasury
Coordinate with:	DOD, NSA, FEMA	NSA	DIB and Private Industry, Stat	State, DIB, USAID	State
Timeframe (yrs)	3	5	5	3	5
Funding Source	DHS	DOD (OSD)	Commerce	DoD FMS Offset Program	US Private industry, with Direct funding from Commerce and Tax Incentives from Treasury
Estimate ($Millions)	$140-160 annually	$100-300 annually for 3 years to qualify more sources.	$1000 ($200mm/yr for 5 yrs)	$1000-2000 per foundry startup (apx 20% of total capex per plant)	$1000-2000 per foundry startup (apx 20% of total capex per plant)
Launch Milestone	N/A	N/A	N/A	N/A	N/A.
Contract Type	N/A. Include in DHS annual budget	To be proposed by DMEA.	Service Contract: Commerce selects program manager to lead standard development with Industry	N/A--Part of FMS contract through State and DIB Platform lead	N/A.
Sustainment Stgy	N/A. Include recurring sustainment funds in DHS' annual budget Disaster Resiliency line item.	Self-sustaining through contracting via DMEA	After 5 years, PM would be funded by annual fees from industry to maintain certification	None required. Funding by private industry	None required. Funding by private industry
Allied Partners	N/A.	N/A	NATO nations; High Tech companies wary of Chinese and Russian supply chain reliability	Target nations: India, Philippines, Mexico, UAE, Brazil, Romania, Japan, Israel, South Korea, Malaysia, EU,	Allied nations in which US Companies have vast reserves of unrepatriated funds.
Iron Triangle Issues	Will require cooperation with State governments, EMS and other first responders	Objections by industry for adding bureacracy, cost, and government-endorsed compeititive mfg source. Possible objections from IBM to the govt's creation of additional sources for TF production	Must coordinate carefully with State to handle delicate issues with RUS and PRC, and to invite them to participate in standard compliance. Some in private industry may complain that a standards implementatition will add costs and disadvantage small business. Small business administration coordination/cooperation will be necessary	Potential political resistance to "shipping jobs overseas";	Complexity of coordination means it will take longer to implement than FMS program. Target companies with unrepatriated funds overseas--give them incentives to invest.
DIB Issues	Will require cooperation of financial institutions, as well as operators of critical infrastructure (Dams, Power Plants, Electrical Grid).	Concerns with price increases, schedule delays and hold-up risk from limited supplier sources.	DIB likely to be very supportive. Will add costs to the acquisition of all systems using MPs/Ics	Scale of foundry investment might mean that a substantial weapon system purchase by target nation is a requirement for Offset program to be attractive. This fact might restrict the opportunity to Tier 1 defense contractors	Scale of foundry investment would require cooperation of very large private companies.

Table 8. Key Programs for Trusted MP Supply

Cyber DefCon/Disaster Resiliency.

The December 2014 cyberattack on *Sony Pictures Entertainment*, apparently launched by North Korean-sponsored actors, exposed the need to establish a national posture and protocol delineating roles and responsibilities for cyber protection and response. When queried by reporters, government officials seemed neither able to articulate which agency (DoD, DHS, NSA, etc.) was responsible for protecting companies from such attacks, nor which agency might be tasked with responding, let alone if the government would assume responsibility for any future defense of industry. The cost of estimated damages to Sony begin at $15 million.[135] Given the cost and psychological impact of the attack, even though no person was injured, had the attack been *kinetic*, the government's responsibility would have been clearer, and its response would likely have been swifter, more resolute and more impactful. Accordingly, Congress should task the Department of

Homeland Security (DHS) to develop, implement and exercise Cyber Defcon and Resiliency procedures, requiring $150 million per year of DHS' $9.6 billion discretionary annual budget for *Disaster Resiliency* to be invested in maturing the competency.[136] DHS would not only negotiate and clarify roles and responsibilities of the various national security agencies, but would also distinguish those accountabilities allocated to the federal government from those left to private business, while also enabling DHS to refine protocols with lessons learned from inter-agency exercises.

Industry Process Standards.

In addition to the threat of malware-infected MPs, studies reveal that counterfeit components comprise 8% of the global supply chain.137 Encouraging and adopting global standards promoting quality assurance, accountable traceability in product custody chains, responsible corporate behavior, respect for intellectual property rights, safe working conditions, competitive fairness and ethical treatment of workers while discouraging counterfeiting, polluting and corruption will serve to level the playing field for all electronics suppliers. Requiring Chinese compliance would reduce cyber risk while also bringing their costs in line with those of more responsible producers.

Ethics Standard: EICC Code of Conduct. The Department of Commerce should promote Support global compliance with the Electronic Industry Citizenship Coalition (EICC) Code of Conduct. The EICC Code of Conduct version 5.0 goes into effect on 1 April 2015. It establishes compliance standards for Labor, Health and Safety and Environmental Protection, Ethics and Management Systems.[138] Insisting on compliance as a requirement for doing business with the US would discourage suppliers from taking shortcuts that artificially reduce costs and create negative externalities such as pollution and poor working conditions, while encouraging respect for intellectual property law, civil liberties, and workers' rights to organize.

Electronics Industry Supply Chain Standard. Without widespread adoption of practices similar to Aerospace Standard AS-9100–a comprehensive vendor certification and audit system which requires quality-oriented management practices as well as documentation, accountability and traceability of each step in the value chain–it will be impossible to impose the supply chain discipline necessary to contain malware-infected or counterfeit components. The electronics industry has been struggling for several years to develop such a standard with only limited traction, primarily due to lack of dedicated funding and no dedicated standards-development leadership. The US Department of Commerce should be funded and staffed to lead and drive standard-development in partnership with industry organizations, leaders in the defense industry, and companies like Oracle, which has developed an internal proprietary process for its own supply chain assurance, as well as cloud-based commercial software for supply chain management.[139] Through its International Trade Administration (ITA) and the National Institute of Standards and Technology (NIST), Commerce could support both the EICC and Supply Chain standards via a reallocation of only 2% of its $9.8 billion annual discretionary budget ($200 million per year, for five years) to ITA and NIST to accomplish this task.[140] The State Department's diplomatic assistance may be necessary to overcome likely Chinese resistance to the implementation of these standards. Domestically, Commerce will need to coordinate with the Small Business Association

(SBA) and Congress to develop programs to assist small businesses with cost and compliance issues in transitioning to the emerging standards.

Trusted Foundry Program.

The Director, Defense Research and Engineering's Trusted Foundry Program[141] should be expanded with a $150-$300 million annual recurring investment to ensure that MPs critical to US weapons and security systems can be surge-produced in the event of an emergency. Through NSA's Trusted Access Program Office (TAPO), any government-sponsored program can access production of integrated circuits through IBM's trusted foundry, provided they can afford the cost and deal with scheduling constraints inevitable when dealing with a single-source supplier. Accordingly, the Defense Microelectronics Activity (DMEA), the Trusted Foundry program manager, should be commissioned to qualify and maintain additional trusted foundries. Concurrently, some of the annual funding should be used to stockpile critical supplies of obsolete MPs that are still utilized in modern systems but which are no longer produced by commercial industry—a critical problem facing defense contractors sustaining high-tech platforms over several decades.

Develop Alternative Foundries in Low Cost Nations.

Foreign Military Sales (FMS) Offsets Supporting Foundry Construction.

Although a domestic Trusted Foundry surge capacity will enhance national security for critical systems, in the face of exploding demand, additional MP sources will be needed to reduce American dependence on Chinese manufacturers. In concert with State and USAID, DOD can encourage the use of FMS Offset programs to seed the establishment of foundries in friendly, low-cost nations who make significant purchases of US defense systems. In nations such as India, such a program would not only encourage a transition from Russian to US weapon systems, it would also provide an economic and security hedge against Chinese regional hegemony while enhancing India's economy at little incremental cost to the American taxpayer.

High-Tech Industry Co-Investment of Un-repatriated Funds.

With key support from State and Treasury, Commerce should develop a program to encourage US companies with un-repatriated funds locked up overseas to invest in startup foundries in friendly, low-cost nations. Such a program would not only reduce our MP dependence upon China and deliver economic benefits to allies, but it would also indirectly direct a portion of the estimated $2 trillion locked-out to the benefit of the taxpayer without changing the politically-sensitive corporate income tax rate.

Conclusion

The combination of US industry's exit from MP production and China' rapid capture of much of the MP value chain represents a mounting threat to American national security. Not only are US defense systems and critical high tech industries subject to potential hold-up risk from Chinese suppliers, they are also vulnerable to hazards from counterfeit parts and malicious, untraceable threats that can be pre-programmed into MP circuitry. Until reliable global supply chain standards are adopted, national security professionals must assume that many of our critical systems and industrial control systems are already compromised. Only a multiple-front, whole of government approach deployed to exploit weaknesses in the Chinese "low-cost-producer" industrial strategy

will cover all of the U.S's vulnerabilities. Accordingly, while the US develops a more robust cyber response posture, alternative competitive and trusted foundry production sources must be developed at home and overseas. Finally offensive, defensive, and game-changing technologies must also be developed and matured to counter the Chinese threat—thereby arming the US with a wide range of options from cyber détente to full-scale, mutually-assured cyber destruction.

Endnotes

[1] Eric Schmidt and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations and Business*. New York: Alfred A. Knopf, 2013, 3

[2] Robert J. Shapiro and Aparna Mathur, "The Contributions of Information and Communication Technologies To American Growth, Productivity, Jobs and Prosperity," *Sonecon*, September 2011, http://www.sonecon.com/docs/studies/Report_on_ICT_and_Innovation-Shapiro-Mathur-September8-2011-1.pdf . p.1.

[3] Atkinson, Robert D. and Luke A. Stewart, "Just The Facts--Economic Benefits of Information and Communications Technology", May 14, 2013, *The Information Technology & Innovation Foundation*, www.itif.org.

[4] Harald Bauer, Mark Patel, and Jan Veira, "The Internet of Things: Sizing Up the Opportunity." McKinsey & Company, Autumn 2014, Accessed December 6, 2014. http://www.mckinsey.com/Client_Service/Semiconductors/Latest_thinking

[5] J. Manyika, M. Chui, J. Bughin, R. Dobbs, and A. Marrs, "Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy." McKinsey Global Institute, May 2013. Accessed December 6, 2014. http://www.mckinsey.com/insights/business_technology/disruptive_technologies

[6] "National Security Strategy," February, 2015. Accessed March 16, 2015. http://www.whitehouse.gov

[7] IBIS World - reports for all NAICS.

[8] OECD (2014), Patents by technology fields, 1999-2011: As a percentage of total patent applications under the Patent Co-operation Treaty (PCT), in *OECD Science, Technology and Industry Outlook 2014*, OECD Publishing, Paris. Referenced April 7, 2015 http://www.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-outlook-2014/patents-by-technology-fields-1999-2011_sti_outlook-2014-graph57-en

[9] IBIS World, "Industry Report 51121-Software Publishing," March 2015, 4. IBIS World, "Industry Report 51913a-Search Engines," December 2014, 4. IBIS World, "Industry Report 51913b- Internet Publishing and Broadcasting," December 2014, 4. IBIS World, "Industry Report 51821- Data Processing & Hosting Services," January 2015, 4. IBIS World, "Industry Report 54151-IT Consulting in the US," December 2014, 4.

[10] IBIS World, "Industry Report 33422 - Communication Equipment Manufacturing in the US," March 2015, 3.

[11] Ibid., 36.

[12] Ibid., 26.

[13] Ibid., 36.

[14] Ibid., 23.

[15] Ibid., 7-10.

[16] IBIS World, "Industry Report 33411A - Computer Manufacturing in the US," December 2014, 8-9. IBIS World, "Industry Report 33461 - Recordable Media Manufacturing in the US," November 2014, 9.

[17] IBIS World, "Industry Report 51721 - Wireless Communication Carriers in the US," March 2015, 2.

[18] Ibid, 4.

[19] Ibid, 4.

[20] IBIS World, "Industry Report 51121-Software Publishing in the US," March 2015, 4.

[21] Annual labor compensation cost for NAICS 51121. Bureau of Labor Statistics. http://beta.bls.gov/dataViewer/view/timeseries/IPUJN51121_L020. Retrieved on March 27, 2015.

[22] IBIS World, "Industry Report 51121-Software Publishing in the US," March 2015, 10.

[23] IBIS World, "Industry Report 54151-IT Consulting in the US," December 2014, 2.

[24] Ibid., 4.

[25] Ibid., 35.

[26] Ibid., 35.

[27] Ibid., 24.

[28] Ibid., 5.

[29] Desilver, Drew. 2014. "Five Years in, Recovery still underwhelms compared to previous ones." *Pew Research Center*. http://www.pewresearch.org/fact-tank/2014/06/23/five-years-in-recovery-still-underwhelms-compared-with-previous-ones (accessed on 8 February 2015).

[30] Ibid.

[31] 2013. *The Economy Watch*. http://www.economywatch.com/economic-statistics/United-States/Output_Gap_Percent_of_Potential_GDP. (accessed on 8 February 2015).

[32] Kendall, Frank. 2015. Eisenhower School. Professional Leadership Series.

[33] "National Security Strategy," February, 2015. Accessed March 16, 2015. http://www.whitehouse.gov, 2.

[34] Ibid, 16.

[35] Annotated in interviews with Cisco, Arista, Oracle, and Facebook. ICT Industry Study Seminar trip March 2015.

[36] Ibid.

[37] Ibid.

[38] Ibid.

[39] Atkinson, Robert D. 2007. "Expanding the R&E Tax Credit to Drive Innovation, Competitiveness and Prosperity." *Journal of Technology Transfer* 32 (6): 617-628. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/203607136?accountid=12686. (accessed on 5 February 2015).

[40] Atkinson, Robert D. 2014. "Understanding the US National Innovation System." The Information Technology & Innovation Foundation. http://www.itif.org/publications/understanding-us-national-innovation-system (accessed on 5 February 2015).

[41] Ezell, Stephen. 2014. "Leveraging ICTs to Bolster European Productivity and Economic Growth." Bridges volume 41.

[42] Atkinson, Robert D. 2014. "Understanding the US National Innovation System." The Information Technology & Innovation Foundation. http://www.itif.org/publications/understanding-us-national-innovation-system (accessed on 5 February 2015).

[43] Ibid.

[44] Ibid.

[45] Strategy&. 2013. "The Global Innovation 1000: Comparison of R&D Spending by Regions and Industries." http://www.strategyand.pwc.com/global/home/what-we-think/global-innovation-1000/rd-intensity-vs-spend-2013-v2stage. (accessed on February 14, 2015).

[46] Ibid.

[47] Mergent Online. http://www.mergentonline.com.nduezproxy.idm.oclc.org/ basicsearch.php. (accessed on February 14, 2015).

[48] Bureau of Economic Analysis. Research and Development Satellite Account. http://bea.gov/national/rd.htm. (accessed on 15 February 2015).

[49] Jennifer Lee and Andrew Schmidt. 2010. Bureau of Economic Analysis. "Research and Development Satellite Account Update." http://search.bea.gov/search?query=Research+and+Development&commit=Go&utf8=%E2%9C%93&affiliate=USbureauofeconomicanalysis. (accessed on 15 February 2015).

[50] Bureau of Economic Analysis. 2013. "Comprehensive Revisions to NIPA: Reconsidering Treatment of R&D and Entertainment." http://blog.bea.gov/category/research-development/page/2. (accessed on 15 February 2015).

[51] Jennifer Lee and Andrew Schmidt. 2010. Bureau of Economic Analysis. "Research and Development Satellite Account Update." http://search.bea.gov/search?query=Research+and+Development&commit=Go&utf8=%E2%9C%93&affiliate=USbureauofeconomicanalysis. (accessed on 15 February 2015).

[52] Ibid.

[53] Ibid.

[54] Robert Shapiro and Aparna Mathur. 2011. "The Contributions of Information and Communication Technologies to American Growth, Productivity, Jobs and Prosperity." Sonecon. https://www.tiaonline.org/.../Report_on_ICT_and_Innovation_Shapiro_Mathur_ September_8_2011.pdf. (accessed on 15 February 2015).

[55] Ibid.

[56] Ibid., 4.

[57] Ibid., 4.

[58] Ibid., 5.

[59] Ibid., 5.

[60] Library of Economics and Liberty. The Concise Encyclopedia of Economics. Robert Merton. Solow. http://www.econlib.org/library/Enc/bios/Solow.html. (accessed on 15 February 2015).

[61] Ibid.

[62] Robert Shapiro and Aparna Mathur. 2011. "The Contributions of Information and Communication Technologies to American Growth, Productivity, Jobs and Prosperity." Sonecon. https://www.tiaonline.org/.../Report_on_ICT_and_Innovation_Shapiro_Mathur_September_8_2011.pdf. (accessed on 15 February 2015).

[63] Ibid.

[64] Ibid.

[65] Ibid.

[66] James Kadtke and Linton Wells II. "Technology Is a Strategic National Security Component." *Signal* 69, no. 5: 27-28. *International Security & Counter Terrorism Reference Center*, EBSCO*host* (accessed February 16, 2015).

[67] Ibid.

[68] Figliola, Patricia Moloney. 2015. "The Federal Networking and Information Technology Research and Development Program: Background, Funding, and Activities." RL33586. (accessed on 16 February 2015).

[69] Weber, *Waiting for Superman how we can Save America's Failing Public Schools* (New York: PublicAffairs, 2010), 263.

[70] Lee, Peter. *Senate Commerce, Science and Transportation Committee Hearing*. 2012. Lanham, US, Lanham: Federal Information & News Dispatch, Inc. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1069247142?accountid=12686.

[71] Hurtado, Sylvia; Chang, Mitch. Degrees of Success: Bachelor's Degree Completion Rates Amongst Initial STEM Majors, Higher Education Research Institute UCLA, 2010. http://www.heri.ucla.edu/nih/downloads/2010%20-%20Hurtado,%20Eagan,%20Chang%20-%20Degrees%20of%20Success.pdf

[72] Gonzalez and Kuenzi, *CRS Science, Technology, Engineering, and Mathematics (STEM) Education: A Primer*US Congressional Research Service, 2013), 1-38.

[73] Ibid

[74] Greenwald, B.; Stiglitz, J.E., Creating a Learning Society: A New Approach to Growth, Development, and Social Progress, Inaugural Arrow Lecture, Columbia University. New York: Columbia University Press, 2014.

[75] Ibid.

[76] Gina Chon. "Cyber Threat Forces Change of Tack at DoJ" Financial Times, January 27, 2015. http://ft.com. Accessed January 27, 2015.

[77] Department of Homeland Security. "About the National Cybersecurity and Communications Integration Center." Accessed April 12, 2015. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

[78] US Congress. "National Cybersecurity Protection Act 2014". https://www.congress.gov/bill/113th-congress/house-bill/3696.

[79] Executive Order – Promoting Private Sector Cybersecurity Information Sharing (2015). https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. Accessed February 14, 2015.

[80] Warren Strobel. "US creates new agency to lead cyberthreat tracking" February 10, 2015. http://news.yahoo.com/u-establish-cybersecurity-agency-official-125311583.html.

[81] Charlie Mitchell. "Exclusive: Obama to Unveil Liability Relief Strategy in Info-Sharing Plan." Inside Cybersecurity, January 30, 2015. http://insidecybersecurity.com.

[82] Michael Rogers, Director National Security Agency, Commander US Cyber Command. Comment to HASC , televised on CSPAN November 20, 2014.

[83] Department of Energy and The GridWise Alliance. The Future of the Grid, Evolving to Meets Amercia's Needs. Decemeber 2014.Page 1. http://energy.gov/sites/prod/files/2014/12/f19/Future%20of%20the%20Grid%20December%202014.pdf. Accessed January 28, 2015.

[84] Barack Obama, Presidential Policy Directive 21. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. Accessed March 25, 2015

[85] Department of Homeland Security. Critical Infrastructure Segments. http://www.dhs.gov/critical-infrastructure-segments. Accessed 25, 2015.

[86] Douglas Ernst, The Washington Times. November 20, 2014. http://www.washingtontimes.com/news/2014/nov/20/nsa-china-has-power-shut-down-us-power-grid-cybera/#ixzz3P04iToD0

[87] Ibid.

[88] Doyle Rice and Alia E. Dastagir. *One year after Sandy, 9 devastating facts*. USA Today, October 29, 2013. http://www.usatoday.com/story/news/nation/2013/10/29/sandy-anniversary-facts-devastation/3305985/ Website accessed January 18, 2014.

[89] Marianne Lavelle. *Can Hurricane Sandy Shed Light on Curbing Power Outages?* National Geographic News. November 2, 2012. http://news.nationalgeographic.com/news/energy/2012/11/121102-hurricane-sandy-power-outages/. Accessed January 20, 2015.

[90] DOD News, USNORTHCOM Update. Pentagon Provides Sandy Response Update. November 9, 2012. http://www.defense.gov/news/newsarticle.aspx?id=118496. Accessed January 18, 2015.

[91] Kayla Webley. Hurricane Sandy By the Numbers: A Superstorm's Statistics, One Month Later. Time. November 26, 2012. http://nation.time.com/2012/11/26/hurricane-sandy-one-month-later. Accessed January 20, 2015.

[92] US Department of Energy. Smart Grid. Energy.gov. http://energy.gov/oe/services/technology-development/smart-grid. Accessed January 28, 2015.

[93] Ibid.

[94] Government Accounting Office. CYBERSECURITY Challenges in Securing the Electricity Grid Statement of Gregory C. Wilshusen, Director Information Security Issues. Testimony Before the Committee on Energy and Natural Resources, US Senate. July 24, 2012. Page 5.

[95] US Department of Energy. Smart Grid. Energy.gov. http://energy.gov/oe/services/technology-development/smart-grid. Accessed January 28, 2015.

[96] Behr, Peter. *Smart Grid Costs Are Massive, but Benefits Will Be Larger, Industry Study Says.* The New York Times, May 25, 2011. http://www.nytimes.com/cwire/2011/05/25/25climatewire-smart-grid-costs-are-massive-but-benefits-wi-48403.html?pagewanted=all. Accessed January 28, 2015.

[97] John Bussey and Steven Rosenbush. "Wall Street Journal Report – CIO Network." February 10, 2015. http://online.wsj.com. Accessed February 12, 2015.

[98] John Bussey and Steven Rosenbush. "Wall Street Journal Report – CIO Network." February 10, 2015. http://online.wsj.com. Accessed February 12, 2015.

[99] National Security Strategy (2015). http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. Accessed February 6, 2015.

[100] "The Federal Information Security Management Act of 2002 ("FISMA", 44 USC. § 3541, *et seq.*) is a US federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347, 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the US.[1] The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." http://en.wikipedia.org/wiki/Federal Information_Security_ Management_Act_of_2002, February 11, 2015.

[101] Jack Moore, "FITARA Analysis: Will CIOs Use Their New Powers for Good?" Nextgov. December 12, 2014. Accessed April 8, 2015. http://www.nextgov.com/cio-briefing/2014/12/fitara-analysis-will-cios-use-their-new-powers-good/101160/.

[102] Ibid.

[103] Richard Walker, "Federal IT Spending Slashed In Proposed 2015 Budget - InformationWeek." InformationWeek. March 5, 2014. Accessed April 12, 2015. http://www.informationweek.com/government/cybersecurity/federal-it-spending-slashed-in-proposed-2015-budget/d/d-id/1114126.

[104] "Open Internet." Open Internet. Accessed April 8, 2015. http://www.fcc.gov/openinternet.

[105] "Statistics." ITU. December 23, 2014. Accessed April 8, 2015. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[106] "Cyberspace 2025: Today's Decisions, Tomorrow's Terrain." Cyberspace2025: Today's Decisions, Tomorrow's Terrain. June 1, 2014. Accessed April 8, 2015. http://www.microsoft.com/security/cybersecurity/cyberspace2025/#chapter-1.

[107] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014–2019. Retrieved on February 22, 2015.

[108] Social Media Engagement: The Surprising Facts About How Much Time People Spend On the Major Social Networks: http://www.businessinsider.com/social-media-engagement-statistics-2013-12#ixzz3RRWEqviC. Accessed on February 1, 2015.

[109] Mark Patel and Jan Veira. "Making Connections: An Industry Perspective on the Internet of Things." McKinsey Insights & Publications. December 1, 2014. Accessed January 15, 2015.

http://www.mckinsey.com/insights/high_tech_telecoms_internet/making_connections_an_industry_perspective_on_the_internet_of_things?cid=other-eml-alt-mip-mck-oth-1412.

[110] "Cyberspace 2025: Today's Decisions, Tomorrow's Terrain." Cyberspace2025: Today's Decisions, Tomorrow's Terrain. June 1, 2014. Accessed April 8, 2015. http://www.microsoft.com/security/cybersecurity/cyberspace2025/#chapter-1.

[111] Wikipedia. Research and Development Efficiency Act. http://en.wikipedia.org/wiki/Research_and_Development_Efficiency_Act. (accessed on 15 February 2015).

[112] The importance of creating innovation clusters is attributed to Michael Porter, Harvard Business School Professor, in the 1990's. Robert D. Atkinson, "Understanding the US National Innovation System." The Information Technology & Innovation Foundation. 2014. Accessed on 5 February 2015, http://www.itif.org/publications/understanding-us-national-innovation-system

[113] O'Donnell, Noreen. 2013. The Financialist. "Subsidizing College Majors." https://www.thefinancialist.com/subsidizing-college-majors. (accessed on 16 February 2015).

[114] Alan Balutis, "FITARA Is Law: Delay Is Not an Option." Federal Times. March 12, 2015. Accessed April 8, 2015. http://www.federaltimes.com/story/government/it/blog/2015/03/11/fitara-law-delay-not-option/70155690/.

[115] Rick Boucher, "Legislative Thaw on Net Neutrality." TheHill. April 7, 2015. Accessed April 8, 2015. http://thehill.com/opinion/op-ed/238141-legislative-thaw-on-net-neutrality.

[116] Mintz, Jack M. and Duanjie Chen, Tax Foundation Special Report, February 2015, no 228. http://taxfoundation.org/article/us-corporate-taxation-prime-reform

[117] KPMG Corporate and Indirect Tax Rate Survey 2014, p 16. http://www.kpmg.com/global/en/issuesandinsights/articlespublications/pages/corporate-indirect-tax-rate-survey.aspx

[118] Wagaman, David D., C.P.A. and Robert E. Duquette C.P.A.. "Corporate Income Tax in Desperate Need of a Makeover." 2013.

[119] Zucman, Gabriel. 2014. "Taxing Across Borders: Tracking Personal Wealth and Corporate Profits." *The Journal of Economic Perspectives 28 (4)*: 121-148. http://dx.doi.org/10.1257/jep.28.4.121.

[120] Dickinson, Tim. 2014. "The Biggest Tax Scam Ever." *Rolling Stone*, Sep 11 2014, 33-37.

[121] "Repatriating Games." 2014. *Shareowner (Online)* 29 (1): 4-5.

[122] http://techcrunch.com/2014/04/28/apple-to-raise-another-17b-in-debt-to-avoid-repatriating-foreign-held-cash/ Accessed 10 Feb 2015.

[123] "Repatriating Games" *Shareowner* (Online) 29 (1): 4-5.

[124] Engel, R., & Lyons, B. "Trapped Cash: When is a Dollar Not Worth a Dollar?" Strategic Finance, 95(10), 2014, 37-43.

[125] Daniel Castro and Rob Atkinson, "'Stim-Novation': Investing in Research to Spur Innovation and Boost Jobs." The Invormation Technology & Innovation Foundation, 27 January 2009. http://www.itif.org/files/2009-stim-novation.pdf

[126] Duguet, Emmanuel. 2012. "The Effect of the Incremental R&D Tax Credit on the Private Funding of R&D an Econometric Evaluation on French Firm Level Data." *Revue d'Économie Politique*, May, 405-435.

[127] Morrison, Michael Ian. 2013. "The Acquisition Supply Chain and the Security of Government Information Technology Purchases." Public Contract Law Journal 42 (4): 749-792.

[128] The Comprehensive National Cybersecurity Initiative. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative, accessed 22 Mar 2015.

[129] New York Times 4 Feb 2010, and www.toyota.jp, accessed 15 Dec 2014.

[130] EE Times, May 14, 2014.

[131] IBIS World China Industry Report, 2014.

[132] Ibid.

[133] Heritage Foundation March 6, 2014.

[134] "NSA Seeks to Build Quantum Computer That Could Crack Most Types of Encryption." *Washington Post*, 2 Jan 2014. http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, accessed 22 Mar 2015.

[135] Frizell, Sam, "Sony Is Spending $15 Million to Deal with the Big Hack". Time, February 4, 2015.

[136] Department of Homeland Security Budget in Brief 2016. http://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf, accessed 23 Mar 2015.

[137] Gilmore, E. T., Preston D. Frazier, Isaac J. Collins, William Reid, and M. F. Chouikha. 2013. "Infrared Analysis for Counterfeit Electronic Parts Detection and Supply Chain Validation." Environment Systems & Decisions 33 (4): 477-485.

[138] Electronic Industry Citizenship Coalition *EICC Code of Conduct version 5.0*. http://www.eiccoalition.org/standards/code-of-conduct/ accessed 22 Mar 2015.

[139] Sources: https://www.oracle.com/applications/supply-chain-management/products.html, accessed 22 Mar 2015; and interview with Oracle management 5 Mar 2015.

[140] The Department of Commerce Budget in Brief Fiscal Year 2016. http://www.osec.doc.gov/bmi/budget/FY16BIB/EntireDocument-WebVersionWithCharts.pdf

[141] http://www.dmea.osd.mil/home.html, accessed 21 Mar 2015.