Spring 2014
Industry Study

Final Report
Information and Communications Technology (ICT) Industry

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

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) 2014

ABSTRACT: Our findings show that the U.S. ICT industry is the leader of the Global ICT industry and is well positioned to support U.S. national security. After assessing the economic health of the industry, we offer recommendations to address the trust challenges raised by government surveillance, improve cyber security, modernize and improve U.S. ICT infrastructure, including the spectrum challenges confronting the U.S. today, and improve the U.S. education system, as well as to improve the U.S. Government's acquisition system.

COL Abdulaziz Saleh Alsaif, Saudi-Arabian Army
Mr. Gene Boedigheimer, Department of the Air Force
COL Rob Collins, U.S. Army
COL Gail Curley, U.S. Army
CDR Mark Imblum, U.S. Navy
Cdre Muhammad Javaid, Pakistan Navy
LtCol Jon L. Halverson, U.S. Marine Corps
Lt Col Colonel George “Butch” Kinney, U.S. Air Force
Mr. Cristiano A. Marchiori, Department of the Air Force
Ms. Katherine Murphy, International Business Machines
Lt Col Sean Murphy, U.S. Air Force
Ms. Sarah Spence, Defense Intelligence Agency
CDR Luciana Sung, U.S. Navy
Dr. James Travis, PhD, Defense Information Systems Agency
COL James (Jim) Turinetti, U.S. Army
COL Forté D. Ward, U.S. Army
Mr. James L. Watson, Department of the Army

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

PLACES VISITED:

Domestic:

National Capital Region

- Computer Sciences Corporation, Reston, VA
- Communications/ Telecommunications Industry Association, The Wireless Association, Washington DC
- USCYBERCOM, Fort Meade, Maryland
- Defense Information Systems Agency, Fort Meade, Maryland
- Department of Homeland Security, Rosslyn, VA
- International Business Machines, Washington DC
- Information Technology Industry Council, Washington DC
- National Telecommunications and Information Administration, Washington DC
- Sprint, Reston, VA
- Software and Information Industry Association, Washington DC
- Verizon, Reston, VA

Eisenhower School Seminar

- Beijing Yueyou Biomed Technology, Co, Ltd
- Federal Communications Commission
- Joint Staff
- Microsoft
- National Security Agency
- New Atlantic Ventures
- U.S. Patent and Trademark Office

Silicon Valley, California

- Andreessen Horowitz
- Apple
- Arista
- Brocade
- Cisco
- Facebook
- Google
- Oracle
- Twitter

International:

Peoples Republic of China

Beijing

- Beijing University
- BDA
- Baidu

- China Mobile
- Garage Café
- J. Capital Research
- U.S. Information Technology Office

Shenzhen

- Huawei Technologies Co
- ZTE
- Tencent

Introduction

The U.S. National Security Strategy (NSS) states: "[our] digital infrastructure is a strategic asset" and is integral to our future economic competitiveness.[1] The Information and Communications Technology (ICT) industry powers the U.S. digital infrastructure, contributing $960B towards the nation's Gross Domestic Product.[2] Furthermore, estimates of the ICT industry's value added ranges between $995B and $1.7T annually.[3,4] The ICT industry drives our nation's economy and prosperity; a healthy ICT industry remains integral to our nation's future success in the 21st century.

Overall, this study reaches three conclusions. First, the U.S. ICT industry will remain a leader in the global ICT community. Our nation's respect for rule of law and intellectual property rights offers a significant advantage over potential international competitors. Furthermore, domestic firms within this industry remain internationally competitive. Proven higher educational institutions and efficient investment networks, which link venture capitalists with ICT startups, provide a significant competitive advantage to our domestic ICT industry. Despite these advantages, there are four significant headwinds which could dramatically erode future U.S. industry leadership: (1) emerging privacy concerns; (2) evolving cyber security challenges; (3) aging infrastructure insufficiently sized to meet growing demands; and (4) a declining science, technology, engineering, and mathematics (STEM) educated workforce.

To develop these assertions, we conducted an extensive review of the ICT industry. Our analysis defined the ICT industry and assessed its current condition. Our analysis identified the competitive structure and health of the major markets, the health of key firms, and the upcoming risks, challenges, and opportunities facing the ICT industry. In addition to the headwinds presented above, we analyzed the implications of the Internet of Everything (IoE), segmentation of the Internet and Internet governance, net-neutrality, and federal government acquisition policies—all recurring themes during the team's two-week field study. Additionally, we identified the opportunities that high-performance computing (HPC) and big data present to our national security and domestic ICT industries. Finally, we assessed the industry's impact on national security, identified potential government roles and responsibilities for new or supplemental regulation/policy to advance U.S. interests, and identified new areas for the U.S. government (USG) to study and assess for future impacts.

ICT Industry Definition

The ICT industry includes everything from television broadcasting and Internet search engines to computer game development and small computer manufacturing. For the purposes of this study, the team decomposed this broad industry to focus on the segments with significant economic and national security implications. The ICT industry, as defined and analyzed by this team, comprises four key areas: ICT components (including user devices), communications and data transportation, processing, and information technology services.

The components and end user device segment manufactures the individual pieces of communications (including wire and cable), computer and networking equipment, and end user devices used in creating the systems that provide complete ICT services to customers.[5] The major firms within this segment typically purchase components from other manufacturing industries and complete product assembly. This segment also includes software publishers who license software for consumer use on end user devices. Key competitors within this segment include Apple, Brocade, Cisco, Hewlett Packard, International Business Machines (IBM), and

Microsoft. International firms, such as Huawei, Samsung, and ZTE, also compete with these U.S. firms for market share. This segment pursues new manufacturing technologies and offshoring initiatives to reduce manufacturing costs, as well as pursuing new technologies to differentiate their products within this highly competitive segment.

The communications and data transportation segment includes wired and wireless telecommunications providers and resellers providing consumers with connectivity for end user devices.[6] The major U.S. telecommunications firms, such as AT&T and Verizon, own and operate their infrastructure and lease capacity from their competitors to fill in coverage gaps. In contrast, the telecommunications resellers, such as TRACFONE, lease unused capacity and compete to meet niche market demands for pre-paid telecommunications access.

The processing segment includes Internet services, search engine, and the Internet publishing and broadcasting industries.[7] This segment of the overall ICT industry provides Internet access and search capabilities, web-based services, webpage design, and subscription services across a variety of media. Firms such as Apple, Facebook, Google, Microsoft, and Yahoo compete with international firms such as Baidu and Tencent for global market share.

The final industry segment includes data processing and hosting services, and ICT consulting.[8] This diverse segment provides everything from data and application hosting to advice on integrated hardware and software solutions. Firms within this sector include consulting firms such as Accenture, Booz Allen Hamilton, and Computer Sciences Corporation, as well as traditional suppliers such as Hewlett Packard, IBM, and Oracle, who provide equipment and services to other IT-related industries.

Current Condition

The U.S. ICT industry contains world-class firms with globally distributed headquarters, research and development, manufacturing, assembly, distribution, and point-of-sale centers. This orientation allows these firms to leverage the world's best STEM graduates who develop new products at globally diverse centers of innovation. This global orientation allows U.S. firms to tailor design, manufacturing, and service processes to take advantage of the best labor rates, gain access to raw materials, and finance these processes with global financial expertise while taking advantage of favorable tax rates. Finally, a global orientation allows U.S. ICT manufacturers to operate in locations with stable economies, good governance, and well-developed infrastructure.

Competitive Structure. A leading industry database identifies 5,246 active ICT global firms.[9] These firms operate in sectors characterized with different competitive models. Many sectors consist of oligopolies and monopolistic competition with large firms dominating. The other market segments engage in competition with many firms. [10,11] The large companies in the ICT industry tend to shed unprofitable and non-core departments to maintain high margins while concentrating on core competencies. Additionally, large ICT companies that enter an emerging-market or decide to improve a parallel business segment use external and internal competitions, and individual research projects to identify new capabilities for developmental funding.[12] Large companies also buy emerging companies to gain access to intellectual property, add market segments, or eliminate a competitor.[13] These trends will continue to influence the ICT industry absent government intervention (i.e., anti-trust concerns).

Health of key firms. The ICT seminar analyzed four firms in detail as representative of the U.S. ICT market. For these firms, we analyzed the employment, revenue, and profit trends of key industry segments via analysis of representative firms from different ICT market sectors: Cisco, Sprint, Oracle, and Google.

Cisco leads the networking equipment sector, but must compete with smaller firms that aggressively target Cisco's products. These smaller firms compete on price (Huawei and ZTE) or product differentiation (Brocade, Arista). Cisco responded by shifting emphasis from the networking equipment manufacturing sector to higher margin sectors such as cloud management platforms and data analytics.[14] Cisco continues to divest product lines and lower headcount as cost-cutting measures.[15] Trends in virtual network software and lower-cost competitors may continue to erode Cisco's revenue. Given these countervailing trends, Cisco could either continue as a leading ICT services company, or lead a declining network equipment sector with pressure on profits as its main products lose meaningful differentiation between lower priced substitutes.

Sprint competes in the wired and wireless telecommunications sectors. Sprint continues in a weak operating position as it continues to generate operating losses due to its limited market share, slow modernization, and contiguous-spectrum shortages.[16] Sprint competes based on price for its main mobile market and attempts to gain share through vertical services (mobile payments/mobile cloud/e.g.).[17] Softbank of Japan purchased Sprint in 2012, providing the capital infusion needed to allow this firm to modernize.[18,19] Similar weakness in the other major firms in the U.S. wireless market could cause at least one wireless firm to fail, be acquired, or merge. The industry sees wireless demand increasing with the projected explosion of the IoE, which may allow the industry to regain some of its pricing power.[20]

Oracle leads the enterprise software market. To enhance its competitive position, Oracle expanded its services to include data analytics and cloud computing.[21,22] While following this product differentiation approach, Oracle's revenues grew slowly over the past several years with profits increasing $1B per year.[23] Oracle maintains a strong margin and cash position, and retains a solid technical footing. Their profits are threatened by intense sector competition and open source big data solutions. Our assessment identifies that Oracle operates with an uncertain future – continual growth in profits, or it may lead a market on the decline as open source competitors take market share and their Sun equipment manufacturing subsidiary continues to be a drag on earnings.

Google, as a world-class information provider, continues to cultivate a diversification of products and services. Google's strategy positions itself as a full service ICT company following cost leader and differentiation approaches depending on its share within diverse market segments. To control costs, Google is vertically integrating its supply chain by adding energy, cable ownership, and equipment manufacturing in order to control operating expenses. These activities resulted in Google's profits increasing $1B+ per year over the past several years.[24,25] Finally, Google continues to look for ways to monetize all aspects of its business, mostly through advertising.[26] Our assessment is that Google will continue to lead its chosen sectors.

Looking at these four firms as a microcosm of the U.S. ICT industry, growth opportunities exist. Companies choose a variety of strategic approaches – market leader/follower – and both cost and differentiation approaches.[27] However, software is vastly more profitable than hardware.[28,29] As a result, U.S. firms move into software wherever possible. USG policymakers must find ways to support the profitability of firms operating in all sectors (including hardware) that are important to U.S. innovation – both now and in the future.

Successful business strategies. The competitive nature of the U.S. ICT industry results in most of these successful firms employing viable business strategies. These successful strategies mean that market leaders make the strategic choices that allow them to position themselves more effectively than competitors.[30] Dean and Company identify three strategic options that allow firms to position themselves in the market – System Lock-in, Total Customer Solutions, and Best Product.[31] Google positions itself as a total customer solutions company that allows customers to reduce costs by adopting Google's full range of Web-enabled applications.[32,33] Apple uses System Lock-in to capture and maintain its competitive position by its use of patents and proprietary technology to increase the value of their products by bonding a customer to their products.[34,35] Oracle uses a Best Product strategy for its flagship database product.[36,37] Verizon and Facebook use a Best Product strategy where they achieve customer loyalty by offering best in class products.[38] Other firms in the ICT market that are underperforming compared with their competitors are not positioned as well. Sprint has not achieved success in any of these strategic positioning choices. Many foreign competitors are not positioned as successfully as U.S. firms. As a result, their governments stepped in and created barriers to prevent U.S. firms from employing products in some foreign markets.[39,40]

Foreign competition. Foreign competition remains a concern. ICT equipment manufacturing in the U.S. declined due to lower prices for foreign components.[41] Some foreign governments imposed restrictions on U.S. exports.[42,43] The U.S. Export Control System further restricts U.S. firms from exporting ICT to foreign countries. The combination of low-cost overseas production and restrictions on U.S. exports of finished goods negatively impacts the U.S. ICT industry. As a result of these factors, China emerged as a near-peer economic competitor to the U.S. Beijing implemented an ambitious ICT infrastructure strategy that will provide 98% of its rural villages with 12 MBps Internet service by 2020.[44] Due to China's ICT emphasis, many Chinese companies compete as low-cost alternatives—but there are security concerns.[45] For instance, Huawei, a direct Chinese competitor of Cisco, has a competitive edge on prices for switch and router hardware.[46] ZTE is already the world's fourth largest handset provider and Huawei the fifth, but security concerns currently limit handset sales in the United States.[47,48,49] Continuing competition across the sector is expected to remain the norm as both China and the U.S. attempt to remove barriers to trade while protecting intellectual property.

Southeast Asian states developed ICT assembly manufacturing skill sets to unseat China by low cost strategy. India continues to reform its economy, focus on innovation, and has made great leaps in software production and Internet application development. Couple India's ICT savvy with its vast untapped potential in human capital, and New Delhi could become a formidable player in the global ICT industry. As long as the U.S. continues to have a sufficient supply of STEM-trained, innovate workers, and puts forth serious efforts in the cyber security realm and in quelling privacy concerns, the U.S. ICT industry will continue to lead the global ICT competition.

Opportunities in foreign producer/consumer markets. U.S. companies continue to pursue offshore manufacturing to lower total production costs.[50] Manufacturing tends to migrate to a lower cost production site as long as it is accompanied by ease of access with well-developed infrastructure, a safe and secure facility, and the availability of components or raw materials.[51] Foreign production of U.S. ICT also creates the opportunity to break into foreign consumer markets, especially China and India. Some companies globally co-locate their research and development (R&D) centers with universities or other sources of talent. Final assembly plants tend to remain in the U.S. where components are assembled with tight security controls.[52] This protects software based intellectual property and assures the integrity of the supply chain.[53,54] Apple currently competes in China, while the Chinese government's censorship policies prevent Google and Facebook from competing.[55,56] As the world's largest potential market, China represents a substantial profit opportunity for U.S. firms.

ICT Industry Outlook

Short-Term Outlook.

The 1-5 year outlook for the U.S. ICT industry is positive, surpassing $1.75T in revenue in 2013 (see Appendix A). The ICT industry accounts for more than 10% of a U.S. economy that exceeds $16T. Several of the ICT industry segments are well positioned to grow at rates above the U.S. Federal Reserve inflation rate target of 2%. Analysts project that the ICT industry's largest sector, ICT consulting, will have revenues of $442B and a Compound Annual Growth Rate (CAGR) of 2.44% in 2019.[57] The wireless communications segment will have a CAGR of 2.84%.[58] Three other ICT sectors highlight upward trending CAGRs: Internet Publishing and Broadcasting (20.28%), Search Engines (8.59%), and Database, Storage & Backup Software Publishing (5.53%).[59] These positive growth trends are attributed to increasing reliance on the Internet for business and personal use, as well as growth in cloud computing, big data, and analytics. The major risks to these positive growth trends remain low cost competition from prominent, ambitious and adaptable ICT firms from China and India, as well as challenges in cyber security and privacy.

In contrast, the Communication Equipment Manufacturing, the Computer Manufacturing, and Wired Telecommunications Segments will not grow, with CAGRs from 2013 through 2019 projected at 1.51%, -3.53%, and -0.42% respectively.[60] The manufacturing segments will contract due to overseas competition and lower labor rates abroad, while the Wired segment will contract due to the global trend towards wireless technology.

Long-Term Outlook.

Based on trends studied, this paper asserts six major trends will shape the U.S. ICT industry over the long-term.

Offshoring. Despite recent re-shoring initiatives by Apple and other ICT manufacturers, domestic firms will continue to offshore manufacturing to lower total cost of production.[61] Due to Chinese demographics, current Chinese labor rates provide a competitive advantage but will increase as labor demand outpaces supply. As a result, the U.S. ICT industry will pursue manufacturing operations in Africa and Southeast Asia, which is in the U.S. national security interest because it reduces security concerns associated with a significant manufacturing base in a near-peer competitor.[62]

Telecommunications convergence. Capital requirements, spectrum shortages, and continued consumer migration to wireless devices will result in the convergence of the U.S. wired, wireless, and telecommunications reseller industries.[63] After convergence, three of four firms will operate and maintain large hybrid networks (satellite, terrestrial, and wireless), which provide ubiquitous access to a robust and modernized telecommunications backbone.

Maturation of International ICT Innovation Centers. China and India will close the innovation gap, which is currently a competitive advantage for U.S. firms. Driven by current investments in ICT infrastructure and the return of U.S.-educated STEM graduates, these nations will establish legitimate domestic alternatives to Silicon Valley, which will temper demand for U.S. ICT consulting and services.

Easing Growth in Wireless and Internet Markets. Current revenues due to exponential growth in developing markets will slow as these markets near saturation over the long-term. U.S. ICT firms must lead the transition to the IoE to maximize revenues over the long-term.

Reduced Demand for U.S. Data Hosting. Technology revolutions in China and India, combined with current Internet segmentation and safe-harbor movements, will reduce demand for U.S. data hosting. These trends will establish viable alternatives to U.S. ICT products and services, which will erode the revenues of U.S. firms within this sector.

Headwinds (Essays on Major Issues)

Our seminar identified four major challenges that if not addressed, will result in loss of U.S. leadership of this economically important industry. The essays that follow analyze in detail four significant challenges faced by U.S. industry and government policy makers.

Privacy in Light of Snowden

In early June 2013, Edward Snowden, an NSA contractor, began to make public, unauthorized disclosures of highly classified information concerning the USG's intelligence surveillance programs.[64] These disclosures shocked and outraged individuals, corporations, and governments around the world. Snowden's disclosures undermined the trust between average citizens and the USG and between customers and companies in the U.S. ICT industry. They also greatly undermined the trust between the U.S. and other nations. As one industry executive stated during our industry study, "Snowden is the elephant in the room."[65]

This lack of trust created several national security issues for the USG. The first issue is the extent to which the disclosures and subsequent efforts at transparency by the USG have harmed the national security of the U.S. and its allies. The second issue is the extent to which the disclosures caused economic harm to U.S. ICT companies. The third issue is the potential harm to the openness of the Internet as major nation-states explore "Balkanizing" it by establishing safe harbor rules for data created in their countries. Collectively, these issues threaten U.S. leadership of the global ICT industry and the future of the Internet. This is significant because an open Internet is essential to the United States' enduring national interests of security, prosperity, values, and international order.[66]

Issue #1 – Impact Due to Outrage.

The outrage of the U.S. public, corporations, and foreign governments and the incomplete picture painted by Snowden's leaks caused the USG to confirm or reveal details about highly classified intelligence activities and to take public steps to curb lawful surveillance activities.

Discussion. Two major programs, the bulk collection and storage of telephone metadata and the collection of electronic communications (also known as the "PRISM" program), are examples of highly classified programs that the USG has had to acknowledge, clarify, and defend due to the unauthorized disclosures.[67] Such disclosures can hurt national security by educating hostile actors on how to evade NSA collection efforts. In particular, PRISM, which targets the electronic communications of foreign citizens located outside of the United States, provided critical information in 54 cases of potential terrorist activity since its inception in 2008.[68]

The first concrete step to restrain surveillance activities occurred on March 27, 2014 when the President announced that he would ask Congress to limit the NSA's authority to collect and store bulk metadata from telecommunications providers.[69] Under this program, which was authorized by the Foreign Intelligence Surveillance Act (FISA), as amended by Section 215 of the USA Patriot Act, and approved in execution by the Foreign Intelligence Surveillance Act Court (FISC), the NSA collected bulk data including "the number calling, the number called, and the date, time, and duration of the call" for all calls originating in the U.S., including those of U.S. citizens.[70] Although all three branches of the USG found this program to be lawful, the public's outrage and the recommendations of two independent USG commissions caused the President to seek to limit the NSA's authority to collect bulk information because of concerns about civil liberties and privacy.[71]

Issue #2 – Industry Impacts.

The ICT industry is confronting three major concerns in the wake of the NSA revelations. First, it faces a trust crisis with outraged customers because the disclosures implied that companies voluntarily provided data about their customers to the USG. Second, it faces a perceived competency crisis amid additional outrage from customers and foreign governments due to the perception that the NSA accesses data that everyone thought was private and secure. Third, the industry faces a business model crisis as foreign governments publicly demand that data be physically stored in their own countries instead of in the "cloud."

Discussion. The CEOs of major ICT companies have met with the President several times since the NSA disclosures began in June 2013. In an effort to rebuild trust with their customers, the CEOs demanded more transparency from the Intelligence Community (IC) and the FISC, including public access to the court orders that required the companies to provide data to the NSA. They are also working to increase and improve encryption of data in order to reassure customers that the NSA and other intelligence agencies do not have access to secret back doors. For example, Google now encrypts search results, although efforts like this have cost millions of dollars.[72] Some, like IBM, are building data centers in other countries, while Microsoft is informing customers that they can store their data in countries outside of the U.S.[73]

Due to a prevalence of multi-year contracts, it is too early to tell exactly how much financial damage has been done to the U.S. ICT industry as a result of the NSA disclosures. However, the early results indicate that the industry is already losing business to foreign ICT competitors and is being excluded from foreign markets. For example, Microsoft lost the government of Brazil as a customer and U.S. companies are not being invited to bid on proposals for foreign customers in Germany.[74] Experts estimate that the industry could lose between $35 and $180B (25% of industry revenue) in cloud computing, web hosting, and outsourcing markets.[75] Industry executives are frustrated by the government's lack of progress on increasing transparency and reforming NSA's programs. As one German software executive noted, "Because of Snowden, our customers have the perception that American companies have connections to the NSA."[76] During our visit to Silicon Valley, industry officials confirmed companies are losing business to foreign competitors, they are spending money to improve security to rebuild trust with customers, and they are frustrated with the USG's inaction and continuing lack of transparency.[77] Likewise, during our visit to China, industry officials said they gained a competitive advantage over U.S. ICT firms due to Snowden's revelations.[78]

Issue #3** – **Regionalization Impact.

The third issue, which is the potential for the regionalization of the Internet, stems from the previous discussion of foreign governments' distrust of data being stored where the NSA could gain access, namely in the U.S. In response, nations such as Brazil and Germany are contemplating laws that would require data to be stored in their countries.

Discussion. Industry is moving towards cloud computing solutions because of the potential to save money. Large and efficient data centers make up the backbone of the global Internet. This model was built on market incentives and is under more scrutiny as governments are viewing data more strategically. They are looking at policies that demand data be stored and processed in-country. Governments are increasingly under more pressure to do something to protect their Internet users and businesses against surveillance. However, the NSA revelations also give them a convenient excuse to further their domestic political and economic objectives. Foreign governments are not thinking long-term about the economic consequences of a fragmented Internet. These short-term, opportunistic types of policies will only make the Internet more expensive and less useful to developing countries and small businesses in the long run.[79]

In the era of the cloud, geographical boundaries should be irrelevant. A requirement to store data in a particular country poses many challenges for U.S. ICT companies. Since the major global ICT companies are mostly US-based, most data is physically stored on servers in the US. Thus, to store data in Brazil would require U.S. companies to build data centers in Brazil even though it does not make economic sense to do so. Additionally, during our visit to Silicon Valley, ICT executives voiced concern about their ability to protect the privacy of foreign users if they are required to store data in countries with immature rule of law or poor records on respect for human rights because, unlike data that is stored in the US, data that is stored in foreign countries would be subject to host nation laws.

Recommendations.

First and foremost, the USG needs to recognize that it has the responsibility, and is in the best position, to mitigate the effects of Snowden's disclosures. It must develop a comprehensive strategy to restore trust in the U.S. ICT industry, the IC, and, ultimately, the Internet. The strategy should focus on:

- Assessment: Understand the problem—loss of trust—caused by Snowden's disclosures and how it impacts the U.S. ICT industry, the economy, and USG/national security.
- Transparency: Educate and engage the public, in a transparent manner, about why the IC collects intelligence (the threat), how privacy is protected in IC activities, and how the USG will be more transparent where it can be without adversely impacting national security.
- Reforms:
    - Internal: Assess and reform overly broad data collection programs; address the insider threat.
    - External: High-level engagement with foreign leaders to restore trust and preserve the openness of the Internet.

The USG needs a strategic communications plan on surveillance and must embrace transparency. The USG issued denials of the worst allegations but has done very little to engage the public or correct the sensationalism in the media's portrayals of leaked information.[80] The USG should begin a dialog with the public to explain why surveillance programs exist, the tremendous safeguards that are in place to protect privacy, and the benefits to national and global security that result from such efforts. It should declassify FISC opinions and Congress should amend FISA to allow the court to hear independent views in cases involving new or significant issues. Americans have a lengthy history of distrusting the Federal Government, and considering that suspicion of government is healthy in a democracy, the USG should respect Americans' discomfort with government surveillance. If the USG wants citizens to trust it, it must earn their trust through dialog, transparency, and, where needed, reforms.

As the President's recent decision concerning bulk telephone metadata collection shows, it is necessary to assess and reform surveillance programs. The IC must be judicious about the type of information it collects and be as transparent as possible on less sensitive matters without jeopardizing particular methods and means of collection. If the IC is employing technology to its maximum effect without consideration of the potential impact to civil liberties and privacy, as appears to be the case in the metadata program, then it needs to step back and reassess the relevance of such information and the potential risks of scaling back such collection efforts.

The NSA revelations also highlight the dangers of the insider threat to national security. As the cases of Bradley Manning and Edward Snowden clearly show, it does not matter how strong external firewalls are if a single empowered individual can download and expropriate reams of sensitive data from the inside. The USG cannot reasonably expect the public to trust it to handle sensitive, privacy centric information with care when it cannot safeguard classified data within its own networks. It needs to reform the security clearance process to ensure that individuals receive only as much access as is necessary to do their jobs. Likewise, it should leverage existing "big data" capabilities to monitor individuals for incidents that might indicate instability (i.e., arrests, visits to foreign countries without proper clearance).

The USG should also carefully consider whether adequate procedures exist so that employees and contractors may communicate concerns about potential fraud, waste, and abuse to a responsive official within the IC. Although Snowden and Manning were not "whistleblowers" within the legal definition of the term, there is a public perception that the IC lacks sufficient avenues for internal complaints.[81] The USG needs to encrypt internal communications and databases so that only individuals with a need to know can access data. It should also use technology to track the movements of individuals within computer networks to identify rogue actors. The USG should also consider in-sourcing all positions in the IC. A contractor should not have access to sensitive, inherently governmental activities like intelligence collection.

The USG must also work with its allies to promote transparency and agree on principles to guide the collection of intelligence in open societies. While the government of Germany has expressed outrage at the NSA's programs, it has also likely been a major beneficiary of the intelligence collected under a variety of programs since 25 of 54 thwarted terrorist plots were in Europe.[82] Many nations rely extensively or even exclusively on the U.S. and its closest allies for intelligence and defense support. They should not be allowed to use the embarrassment of Snowden's revelations and public outrage as an opportunity to help their own domestic ICT companies at the expense of the U.S. ICT industry. Nor can the USG allow other nations to make inflexible demands for safe harbors of data at the expense of the openness of the Internet. Thus, the President should engage in a high-level, concerted effort to persuade foreign senior leaders that their statements and actions can have long-term, adverse consequences for the free flow of information and commerce around the world. These leaders should also embrace transparency in their own countries and seek to educate their citizens on surveillance programs. The principles and values articulated in Presidential Policy Directive 28 are a good starting point for this engagement.[83]

Cyber Security

Malicious cyber activity poses a significant threat to U.S. national security. The cumulative effects of cybercrime and cyber espionage on the U.S. economy represent a dampening of real economic growth. Cyber-attacks threaten critical infrastructure, essential services, and the availability of our most sensitive networks. Admiral James G. Stavridis, NATO's supreme allied commander for Europe and commander of U.S. European Command, told the Senate Armed Services Committee "Today, we have a billion devices that are accessing the Internet. Our economies are entangled in this Internet sea, and it's an outlaw sea. Nothing exists in the norms of behavior. There is a military aspect to it, but it's all of society. At some point, there needs to be a very global conversation on this challenge."[84]

The U.S. faces a spectrum of options in addressing these cyber threats, from leaving the responsibility to individual stakeholders to strictly regulating and enforcing cyber security standards. The individual stakeholders operate, manage, and benefit from the cyber domain and should be very interested in taking precautions, but often underestimate the risks.

Malicious cyber activity is unique when compared to other threats to national security. The following characteristics make it complex as a national security issue.

Issue #1 - Intense Debate.

The cause and effect relationship between malicious cyber activity and the loss of intellectual property, for example, can be tenuous. It is rarely fully understood by the layperson. In fact, unless one has had their identity stolen or their bank accounts illegally accessed, and has paid a significant price due to the event, one likely will not appreciate cybercrime as a national security issue. Until a company "sees" that a breach in their cyber security resulted in direct loss of competitive advantage, it will not likely appreciate cyber espionage as a threat to its future existence. Until the nation experiences a cyber 9/11, i.e., an attack that causes widespread shutdown of an essential service, it will not likely appreciate cyber warfare as an existential threat. A lack of clear cause and effect masks the real dangers.

Issue #2 – It is All Around Us.

Individual, organizational, and governmental activity in the cyber domain was initially a choice. Participation in cyberspace today, either active or passive, is involuntary. Driving a car, educating, managing money, communicating, voting, or paying taxes all require activity in the cyber domain. It will soon be impossible to opt out or go off the grid.

Issue #3 – It Manifests in Many Ways.

Unlike a nuclear weapon that manifests immediately through a large explosion and massive radiation, malicious cyber acts can be subtle and latent. Furthermore, it can reveal itself in loss of intellectual property (IP), theft of money and identification, denial of essential services, loss of privacy, and loss of institutional confidence, among others.

Issue #4 – It is the Result of Multiple Participants.

Cyber criminals and attackers run the gamut from individuals and non-state actors, to state-sponsored actors and nation states. Unlike the nuclear threat or major theater war, where only a few have the capability, those capable of acting maliciously in the cyber domain are numerous and come in all shapes and sizes.

Issue #5 – It is Difficult to Attribute.

Determining specific and meaningful "fault" for malicious cyber activity is difficult for many reasons. Two already discussed are the complex nature of cause and effect and the multiplicity of actors. Additional difficulties arise because cyber activity easily crosses traditional boundaries like national borders; the effects can be latent for many years before anyone detects the damage; and finally, the sheer amount of activity makes it almost impossible to distinguish malicious from benign behaviors.

Issue #6 – It is a Public Good.

A public good is commonly defined as one that is *non-excludable* and *non-rivalrous*, often susceptible to the "*free rider*" problem, and lends itself to excessive use leading to negative externalities.[85] Cyberspace is non-excludable; in fact, we are all either active or passive participants. Cyberspace is non-rivalrous; when one participates in cyberspace it does not prevent another from doing so. On the contrary, when more participate in it, it compels others to do so. Cyberspace is susceptible to the free-rider problem; i.e., entities will avoid contributing to protect cyber space because they not need to do so to benefit. Free-riding in cyberspace results in rampant cybercrime, espionage, and warfare. The Target failure is an example of this. Despite knowing about security weaknesses, they took no action, creating an estimated $240M to $2.2B in costs.[86]

President Obama's administration recently released its *Framework for Improving Critical Infrastructure Cybersecurity*, which states, "The Framework was created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk."[87] But this executive order lacks any enforcement mechanism and is, in fact, voluntary and simply serves to articulate the issue. The President's Cybersecurity Framework is little more than a first step, and will require follow on legislation to generate a real impact.

Public and private sector cyber security spending approached $75B in 2013 ($10B in government spending) with most analysts forecasting between 5-10% growth in each of the next five years.[88] Spending is largely uncoordinated between individual, corporate, public and private entities. Both the Ponemon Institute and Bloomberg estimated in 2012 that to defeat 95% of malicious cyber activity, spending on cyber security would have to grow by a factor of nine.[89] The direct costs of maintaining the status quo are estimated to be more than $300B a year (primarily due to the loss of IP), representing more than 1.5% of GDP.[90]

The current administration's first step for cyber security was to offer a voluntary framework for cooperative improvement. Economics and human nature will put many obstacles in its path. As long as people fail to see cyber security as a necessary "public good," it will continue to be underfunded at all levels. Opponents to cyber security regulations argue that legislation will significantly curtail productivity and innovation. Eventually, pressure from the public will force more action from corporate boardrooms and government agencies. Hard choices may be costly and unpopular, but the cyber domain is "too big to fail." Most of the nation just does not realize it yet.

Recommendation.

Leadership, both corporate and governmental, must drive a comprehensive, prescriptive, and binding framework for cyber security in the near term. Successful domestic cyber security regulation will serve as an example to U.S. global partners and competitors. Further, that commitment will bolster U.S. efforts to create partnerships that curb the incentives, and increase the penalties, for committing malicious cyber activity.

Infrastructure

The U.S. will continue to rely on the ICT industry to provide the telecommunications paths that power our digital way of life. Future network demands will continue to increase as the IoE matures and the variety of on-line resources and subscription services broadens. The wired telecommunications segment operates and maintains our cable infrastructure, which provides fixed broadband access to our homes and offices and backhauls wireless communications to ease congestion on the wireless infrastructure. The wireless telecommunications segment operates and maintains the wireless infrastructure to connect our smartphones and other wireless devices.

Both segments face two near term challenges, which threaten their ability to satisfy future consumer demands.

Issue #1 – Insufficient revenues to sustain and modernize the wired telecommunications infrastructure.

Industry experts suggest the revenues within the wired telecommunications will continue to contract through 2019 for three reasons. First, firms within this market have reduced margins to preserve shares in this intensely competitive market. Second, reduced consumer demand for analog telephony and migrations to wireless services erodes market revenues, though large market competitors mitigate this impact through expanding broadband and on-demand services. Finally, near market saturation limits additional opportunities for growth.

However, to meet this growing consumer demand for digital services, firms within this market must invest in modernization of their infrastructure. Existing copper infrastructures are insufficient to meet digital demands without capital investment in new networking equipment. Furthermore, transitioning customers to a fiber-optic infrastructure, such as Verizon FiOS or AT&T's U-verse, also requires significant capital investment, with low rates of return in all but the wealthiest and most densely populated areas. However, the contraction of operating revenues will either discourage firms from making further infrastructure investments or lead firms to underinvest in infrastructure modernization. In either case, the viability of the nation's terrestrial network to support growing consumer demands is questionable.

Issue #2– The Spectrum Crunch.

Consumer demand for wireless telecommunications services will continue to expand due to a growth in online video consumption, the maturation of the "Internet of things," and an increase in the number of customers who have "cut the cable."[91] Analysts expect the number of wireless devices to reach 50B globally by 2020.[92] However, to communicate, these devices all rely on spectrum, which is a finite resource. Furthermore, not all spectrum allocations are equal.

Large data packets and the need to penetrate environmental obstacles make some spectrum allocations more suitable to wireless telecommunications providers than others. Government requirements, such as defense and law enforcement, further reduce the amount of usable spectrum that is available to our domestic infrastructure. Without additional spectrum blocks or technological innovation that increases the spectrum efficiency of wireless devices, the ability of the wireless telecommunications to meet future consumer demands is also questionable.

Issue #3—The Spectrum Crunch Abroad.

Like our domestic wireless infrastructure, wireless infrastructures abroad also face spectrum challenges and growing pressure from consumer demand. In key regions, such as the Asia Pacific and developing nations, exponential growth in wireless demands limits the amount of spectrum available. This congestion, exacerbated by different allocations, increases the difficulty of getting the right spectrum for military exercises and operations.

Recommendations.

To ensure our domestic telecommunications infrastructure can meet future consumer demands, the federal government should pursue the following policy recommendations.

- Ease net neutrality policies to allow wired and wireless telecommunications providers to counter free rider dynamics within the market, and charge premium content providers based on bandwidth usage.
- Incentivize the modernization of our wired telecommunications infrastructure. This can be accomplished through reducing price caps to allow firms to generate additional revenue for modernization projects, or through the easing of government-imposed tax and fee structures to offset modernization costs.
- As a Federal Communications Commission (FCC) representative recently stated, "No single action is a silver bullet when it comes to meeting mobile capacity needs…more efficient use of spectrum, new technologies, and unleashing new spectrum are all important parts of the mix."[93] The USG should fund R&D to identify new technologies that will use existing spectrum more efficiently, as well as transition spectrum authorizations from the public to the private sector in total, or through a public-private partnership to share infrequently used spectrum authorizations.
- Recognize our digital infrastructure as a public good and invest in its modernization to ensure it can meet future consumer demands.
- Engage with allies to ensure spectrum availability for military operations.

ICT Workforce & Innovation Capacities

U.S. ICT companies have an unparalleled, proven record of innovation and success in the global ICT industry. Companies in the Silicon Valley ecosystem anticipate future trends and nurture human talent at unprecedented levels. The industry enjoys a wealth of highly trained, visionary computer scientists and engineers who are the engines that drive Silicon Valley's success. Yet, despite this success, there is a widely held perception in the media and in academia that the U.S. does not have enough STEM graduates. Without exception, the companies we visited share this belief and are concerned about the future competitiveness of the U.S. ICT industry. Thus, it is important to understand why there is a shortage of STEM graduates, the implications for U.S. national security, and options to remedy this deficit.

***STEM Workforce Shortfalls*.**

It is difficult to determine whether the number of trained STEM workers is adequate for U.S. industrial and government demands. During our survey visits to both industry and government organizations, we learned that many college students would rather major in non-STEM disciplines because they believe other majors to be easier than the hard sciences. Of those students who choose to major in STEM, experts estimate that only 40% actually end up earning a STEM degree.[94] However, we also heard that many STEM graduates opt to pursue non-technical jobs, such as in the financial industry or in sales, because the compensation is higher than in pure STEM jobs. Thus, they use their STEM education as a launching pad to pursue other more lucrative opportunities.

The unemployment rate for STEM professions is very low compared to the unemployment rates for other types of jobs. According to the Bureau for Labor Statistics, the unemployment rate for STEM professions is less than 4% compared to almost 7% for the overall U.S. economy.[95] The U.S. ICT industry has also used the H-1B visa program in order to hire qualified foreign STEM workers. In 2013, U.S. companies submitted over 124,000 visa applications for 65,000 allowable visas. Amazingly, this volume occurred in just the first five days of the program opening for 2014.[96] ICT companies want Congress to authorize more H-1B visas to help alleviate the shortage of qualified technical workers in the U.S.[97]

Implications for U.S. National Security.

Both industry executives and government officials are concerned that a lack of STEM graduates will cause the U.S. to fall behind other nations, such as China, that are growing large numbers of STEM graduates. The U.S. needs STEM graduates to lead the U.S. ICT enterprise, including government, into the 21st century. The challenges of cyber security, big data, HPC, and a host of other complex issues require a technically competent workforce.

A major reason for the U.S. ICT industry's success and leadership in the global ICT industry is that it invests enormous amounts of time and money into R&D inside the U.S., and it largely outsources manufacturing to other countries to save money. If the U.S. continues to experience a shortage of qualified STEM workers, it may be unable to conduct effective R&D in the U.S. If, due to this shortage, the industry has to move R&D outside the U.S., there are serious threats that could harm or impede such work, including industrial espionage, rule of law challenges with respect to intellectual property and trade secrets, and other regulatory, legal, or political roadblocks. Such impediments would cause the pace of U.S. innovation to slow. Over time, the U.S. ICT industry could lose its leadership role in the global ICT industry.

If U.S. R&D moves offshore, the USG would also lose the advantages it enjoys in the national security realm from the access it has to the cutting edge technology that U.S. ICT companies develop. ICT technology is constantly evolving and the U.S. national security establishment must stay one step ahead of rival actors. In addition to losing access to cutting edge technology, the USG needs qualified STEM graduates in order to protect the nation from cyber threats and to develop policies and programs to deter such behavior. By 2016, over 30% of the federal workforce will be eligible to retire.[98] In the next ten years, the USG must recruit and hire STEM graduates to replace employees who retire. While the USG can contract for certain functions, it cannot resort solely to contracting instead of building its workforce because many critical functions are inherently governmental. Thus, like the ICT industry, the USG has important equities in ensuring that the U.S. has enough STEM graduates to meet demands across the private and public sectors.

Options to increase the number of STEM trained workers.

There are several options to increase the number of STEM college graduates and STEM trained workers in the U.S. This is an area where government and industry can work together. As a starting point, the USG should work with industry to develop a national goal that will inspire children and young adults to pursue STEM studies. Ideally, such a goal would be akin to President Kennedy's declaration in 1962 that the U.S. would put a man on the moon by the end of the decade. Beyond such a lofty goal, the USG should pursue short-term actions to alleviate the immediate shortage of STEM workers, and long-term actions to reverse the perceived decline in U.S. students deciding to pursue STEM degrees.

Congress should institute major reforms to the H-1B program. First, it should increase the number of visas available each year from 65,000 to 100,000 or more.[99] Second, it should offer resident alien status to foreign workers who successfully complete an initial H-1B term of three years. Currently, unless the worker asks for a single three-year extension, he or she must leave the U.S.[100] While this has greatly helped the ICT industry in India and other countries, it does not make sense to train foreign workers and then send them immediately home, particularly when they would like to stay in the U.S. The STEM field is of critical importance to U.S. national security; proven H-1B workers should be allowed to stay in the U.S. indefinitely.

With respect to the looming shortage of skilled STEM workers for the USG, the government should step up its recruiting efforts at colleges and universities. It should also offer incentives such as student loan repayments to STEM graduates who agree to work for the USG for a set number of years, just as it currently does for other professions. While the government will never be able to compete with the private sector in terms of pay, it provides unique opportunities for people to learn and acquire responsibilities much earlier in their careers than in industry. It also provides a chance for the best and brightest students to make an immediate impact on national security, which is something that should appeal to many people.

Long-term, government and industry must work together to improve the availability and quality of STEM opportunities in primary and secondary education. This should start with a commitment to improve public schools. It requires purpose, vision, and money. A public-private partnership is the ideal way to empower schools to broaden their curriculums and improve their technical capabilities. Several of the companies we visited have created programs such as "hackathons" to expose children to computer science. These programs, most of which are privately funded, are an excellent way to bring STEM to children and to encourage girls and minorities to consider STEM careers. Governments should seek to partner school districts with industry to these ends. Ultimately, the USG should work with industry and academia to lead a national discussion on the importance of STEM education to the U.S. economy and national security, and how to best allocate scarce resources in support of it.

Conclusion.

The U.S. needs to address the perceived shortage of qualified STEM workers in the labor force. Short-term fixes such as reforms to the H-1B visa program can help, but ultimately the nation must invest in its public schools in order to inspire the next generation to embrace STEM disciplines. Both industry and government require qualified STEM workers in order to compete effectively and to protect national security. This is an area where industry and government can and should work together to develop solutions and to inspire Americans to pursue STEM studies.

Other Challenges for the ICT Industry & USG

Internet of Things (IoT) and the Internet of Everything (IoE). Projections identify the IoE as the next transformative technology. In the IoE, objects ranging from everyday articles to major systems become self-aware through built in processing, and communicate with elements of the wider world via extremely low power networked radios. The U.S. challenge in competing in this industry comes from the non-integrated, fragmented U.S. networking industry and privacy concerns. Appendix B contains additional data and policy recommendations for the IoE.

Acquisition. Technology increases so quickly that the ICT industry often delivers systems to the USG with dated or obsolete components. Where the private sector can work through the process in days or months, the USG procures and fields in terms of months and years. The USG acquisition system cannot keep pace with technological changes. The section on Government Oversight Roles, beginning on page 17, and Appendix B contain additional discussion and policy recommendations for the USG concerning ICT acquisition.

Net-neutrality. Net neutrality is a contentious issue that pits consumers and content providers against the wired and wireless industries. Both sides have valid arguments – the key issue for policy makers is this – who gets first priority to innovate – the wired and wireless industries by developing premium priced quality of service products or the content providers. The outcome of the FCC's current rulemaking efforts could have enormous implications for the future of the Internet and the ICT industry. Appendix B contains additional discussion and policy recommendations for net neutrality

Social media. Social media has been a source of growth for the U.S. and global ICT industry. Policy decisions have limited the employment of social media within the USG and the national security ICT system particularly. The USG should reexamine its policies for social media and find ways to expand its use in all aspects of day-to-day activities. Appendix B contains additional data and policy recommendations for the USG concerning social media.

Opportunities Facing the ICT Industry (Essay on Major Issues)

While challenges exist for the U.S. ICT industry, advances in technology provide opportunities for growth. Of these opportunities, Big Data and HPC provide near term opportunities for the USG and should be vigorously exploited.

Big Data and HPC

Big Data and HPC remain significant opportunities for our domestic ICT industry and the USG. As business and governmental enterprises grow, experts estimate they collect and store 2.5 quintillion (2.5 x 10^{18}) bytes of data on a daily basis. According to IBM, these enterprises created 90% of the data stored in the world today within the last two years.[101] These large, often unstructured data sets, are known as “big data.” Big Data is outpacing traditional computing and data analytics tools. The ability to efficiently and effectively use all of this data could transform the national security enterprise and a wide range of communities including finance, marketing, medical, and R&D.

To exploit this opportunity, the U.S. ICT industry must develop innovative software and hardware solutions across four dimensions to gain a competitive advantage. First, these solutions must efficiently process a large *volume* of a *variety* of both structured and unstructured data.[102] Second, solutions must account for time sensitive imperatives. For example, one financial firm invested $300M to establish a direct connection between financial centers, increasing communications *velocity* by five microseconds - achieving a clear competitive advantage in financial transactions.[103] In addition to volume, variety and velocity, effective solutions must ensure a high level of *veracity*, eliminating false positives and statistical errors, reducing misinterpretations of data.[104] By developing innovative data algorithms that effectively and efficiently address these four dimensions, the U.S. ICT industry will become a world leader in big data solutions and gain significant share of the international market.

HPC represents another opportunity for the U.S. ICT industry to manage the explosion in data generation. HPC relies on massive parallel processing hardware, sophisticated architecture, and highly complex software applications to process large, complex data sets. Governments and corporations continue to drive significant demand for these supercomputers, which simulate reality and model complex designs to develop artificial intelligence, study human genetics, conduct a variety of traffic analysis, search for energy, and refine weather forecasts.[105,106,107,108] Despite growth in HPC capability in both China and India, the U.S. ICT industry's unmatched experience with supercomputing and recent investments by the Defense Advanced Research Projects Agency (DARPA) should provide a competitive advantage, and allow the industry to take advantage of this opportunity.[109,110,111]

Combined, big data and HPC represent a significant opportunity for the USG. Potentially, these areas could transform our intelligence community, where the amount of data collected routinely outstrips our national capacity to process, exploit and disseminate it in a timely manner.[112] As the U.S. NSS recognizes, our "safety and prosperity depend on the quality of the intelligence we collect, the analysis we produce, and our ability to evaluate and share this information in a timely manner."[113] In addition to intelligence, big data and HPC could potentially benefit major weapon system acquisition by reducing design and test cycles, yielding cost savings, and improving design quality and weapons system safety.[114,115] By simulating reality, these systems could provide decision makers greater fidelity on a wider range of options more rapidly.

Government Oversight Roles

The international community witnessed extraordinary development, productivity growth, and increased globalization throughout the Information Age. As a result, Internet management and information distribution became a vital underpinning of the global security domain. However, ICT requires government oversight to properly achieve seamless interoperability and protection, enable the distribution of data and intelligence, and ultimately support the generation of knowledge. The U.S. is faced with a clear opportunity to improve oversight in the form of domestic ICT governance, the promotion of global ICT standards, and reforming USG ICT acquisition processes.

Domestic Oversight. During the ICT team field studies, industry and government agencies both expressed the need for some level of government oversight in the information domain. Industry believes governance should focus more on a general compliance framework, but not mandate specific protocols and standards. ICT oversight, in any form, must accomplish the following objectives: (1) mitigate public safety concerns while balancing security with personal liberties; (2) establish and maintain laws that enforce property rights; (3) mitigate or eliminate the harmful aspects of competition not in accordance with existing U.S. laws; and (4) provide an education system that trains Americans and industrious people of the world to fill roles in the ICT industry.

Governance and Oversight Benefits. Prescribing data and network standards that are proven information assurance "best in breed," and that are continuously verified through security testing, will achieve far-reaching benefits for the U.S. and its national security. Effective governance can safeguard individual privacy, harden network security, and deepen protection measures. The avoidance of poorly protected hardware and software environments can ensure high confidence in authenticity, verification, and unauthorized compromise. In addition, the use of common and interoperable security standards will better facilitate the exchange of network status information, protection files, virus definitions, and the information required to manage and contain attacks, denial of services, and malicious virus files.

Prudent governance will also lead to cost avoidance and savings. Last year, worldwide ICT spending approached $3.6T, with overall annual growth slowing to 3.9%, and only about $40B directed to U.S. Department of Defense (DoD) agencies[116,117] The DoD Chief Information Officer (CIO) anticipates that prudent governance and consolidation within the DoD could recover approximately $3.2B to $5.2B dollars across the future budget window.[118] Extending meaningful oversight throughout the private sector will require both leadership and a unique public–private partnership that balances national security imperatives with innovation, productivity, and privacy concerns.

International Governance. The global economy, free trade ideals, and the exchange of ideas and values are all enabled by the free flow of data. Distrust amongst nations, particularly in the cyber domain, threatens this exchange. Safe harbor rules, rampant theft of intellectual property, cybercrime, and cyber attack are all exacerbated by the absence of meaningful international accords. In fact, the U.S. is at odds with long-standing allies on how data is managed. U.S. global leadership on this matter must occur, and will be considered more credible if it can achieve prudent ICT governance domestically.

National Security Acquisition Reform. A more detailed and focused analysis of the DoD ICT acquisition and governance system lends itself to several observations and recommendations that could benefit system procurement and deployment.

The system must emphasize and incentivize less expense, but effective, options like technology refresh; a continuous cycle of funding allocated for modernization and preplanned product improvements; operations and development testing that enables the adoption of new technologies; and embracing test-fix-test cycles that produce qualified upgrades in two years or less.

Users, policy makers, and combat developers must align requirements with an approach to better leverage and procure commercial technologies. All too often, the user community begins with generic requirements, only to get caught up in a requirements creep phenomena that leads to military unique and development intensive efforts. The DoD historically spends an inordinate amount of time trying to pursue fringe capabilities that often provide very minimal benefit. Combat developers should instead work with the appropriate program team, industry members, and test community to explore existing commercial ICT capabilities ("Commercial Off-the-Shelf" or COTS) and work toward improvements through technology insertion over time.

The system should pursue more technologies that support the employment of spectrum efficient and agile systems where there is global competition for spectrum. Spectrum is a finite resource and the radio frequency bands are reaching historic global levels of saturation. Coupled with the dramatic increase in wireless devices, industry and DoD must collectively work to advance technologies and concepts. In addition, the U.S. Department of State must continually engage, with DoD and Department of Commerce support, in global spectrum governance activities to protect U.S. national security frequency needs. There are compression schemas, multiplexing, and spectrum agility approaches that can greatly enhance our expeditionary, mobility, and geographic spectral freedoms.

With respect to USG acquisition reform, the system must not default to Lowest Price Technically Acceptable (LPTA) contracts for ICT procurements.[119] This creates friction with industry and generates unintended consequences of cheap products and services. During our field studies, industry officials repeatedly stated that they did not want to even submit proposals in LPTA procurements because it was not worth their time.[120] A revision of Better Buying Power (BBP) policies must reinforce that the USG desires best value, even if an increased short-term investment is necessary to obtain larger and longer-term savings.

Finally, advancing ICT governance will require significant improvement on training the workforce and military members on ICT technology. We historically rely on formal training environments that use centralized approaches, dedicated school instructors, and training schedules that orient on a full time student status. More focus is needed on decentralized training concepts that allow the workforce to familiarize themselves with the ICT capabilities more closely to the site of deployment. Local training is a proven technique to help students learn, absorb skills, and develop procedures that make them more productive and proficient on ICT systems. As we work to rapidly field new technologies and expand our capabilities, training and proficiency is the cornerstone that will allow us to maintain efficiency in the employment of ICT capabilities.[121]

Conclusions & National Security Policy Recommendations

Today we are familiar with “things” connected to the Internet: computers, phones, aircraft engines, cars, refrigerators, thermostats, etc. Imagine a future where “everything” is connected. Farms that embed sensors in every plant to measure position, moisture, acidity, and sunlight.[122] A health care industry that mandates the use of wearable medical devices that support preventative medicine.[123] A wireless topography where every device is a public or private “hotspot.” We are already awash in data but lack the tools to use it in a timely manner. CSC predicts that between 2009 and 2020, data growth will compound 44 times.[124] Cisco predicts that the IoT today connects 12.5 billion devices, and that the IoE will connect 50 billion devices by 2020.[125]

It is possible that data could become a personal, organizational, and national security liability if the U.S. does not take significant steps. The future presents immense opportunities for the ICT industry, but also presents obvious national security challenges that we must address. As the President said, the U.S. is “the nation that invented the Internet that launched an information revolution that transformed the world” and “will do what we did in the 20th century and lead once more in the 21st.”[126] To maintain the U.S. position of leadership, this seminar concludes that the policy recommendations in Table 1 be considered and implemented.

Table 1. Policy Recommendations

Issue	Policy Summary/Recommendation
Cyber security	Establish prescriptive cyber security regulation for all U.S. cyber ecosystems.
	Promote enforceable international intellectual property protections.
Privacy protection	Embrace transparency by public discussion of surveillance practices.
	Declassify FISA Court opinions and other key documents.
	Amend FISA to empower the FISA Court to use independent advocates in cases concerning novel issues such as bulk surveillance and to call on expert witnesses from outside of the USG.
	Review existing surveillance programs to ensure that they are narrowly tailored and adequately protect privacy interests.
	Reform security clearance procedures, monitor personnel on networks; encrypt information within USG networks; in-source contractor billets in the IC; and ensure that adequate mechanisms exist for internal privacy and civil liberties complaints.
	Engage foreign leaders to restore trust and to move towards common standards for surveillance such as those articulated in Presidential Policy Directive 28.
ICT governance	Increase emphasis on COT vs. military unique solutions; shorten development.
	Employ 'best value' vs. 'lowest price' contract approaches.
	Employ iterative testing to accommodate pre-planned product improvements.
Infrastructure	Incentivize infrastructure modernization via tax reform.
	Invest in R&D to find new technologies to efficiently use spectrum.
	Ease net neutrality policies to allow carriers premium services.
STEM	Partner with industry to increase the number of STEM qualified individuals.
	Increase the number of H-1B visas for programmers to 100,000+ annually.
	Offer resident alien status to workers completing an H-1B term of three years.
	USG should increase incentives for recruiting of STEM students.
	Pursue public-private partnerships with primary and secondary schools to improve the availability and quality of STEM education.

Appendix A. Tables and Figures

The IBIS database identifies 29 different industries that are part of the ICT market. This database was analyzed and key indicators are summarized in table A-1[127]

Table A-1. ICT Industry Financial Summary by Industry Segments

Industry Segment	IBIS number	2013 Revenues (billions)	2013 Industry Value Added (billions)	% VALUE ADDED	Employees	Revenues per employee (thousands)	2019 Projected Revenue	CAGR
Design, Editing & Rendering Software Publishing	51121d	$10.00	$8.4	84%	66,341	$151	$10.9	1.50%
Operating Systems & Productivity Software Publishing	51121a	$38.60	$28.9	75%	96,321	$400	$53.6	6.48%
Satellite Telecommunications Providers in the US	51741	$6.10	$4.0	66%	14,301	$427	$7.4	3.55%
Data Processing & Hosting Services	51821	$86.40	$54.2	63%	478,278	$181	$105.5	3.68%
Business analytics & enterprise software publishing in the US	51121c	$26.90	$14.5	54%	36,484	$737	$33.3	3.97%
Internet Service Providers	51711d	$53.40	$27.4	51%	221,849	$241	$61.5	2.53%
Database, Storage & Backup Software Publishing	51121b	$38.60	$17.8	46%	61,098	$632	$51.4	5.53%

Industry Segment	IBIS number	2013 Revenues (billions)	2013 Industry Value Added (billions)	% VALUE ADDED	Employees	Revenues per employee (thousands)	2019 Projected Revenue	CAGR
Cable Providers in the US	51711a	$84.30	$38.5	46%	199,765	$422	$90.5	1.23%
ICT Consulting	54151	$385.81	$174.23	45%	1,779,835	$217	$442.34	2.44%
Security Software Publishing	51121f	$9.63	$4.3	44%	21,740	$443	$11.1	2.55%
Internet Publishing & Broadcasting	51913b	$23.50	$10.4	44%	72,346	$324	$52.1	20.28%
Radar & Satellite Operations	51791b	$2.10	$0.9	43%	7,759	$271	$2.3	1.59%
Video Game Software Publishing	51121e	$13.22	$5.7	43%	81,770	$162	$17.3	5.17%
Wired Telecommunications Carriers	51711c	$107.49	$39.0	36%	282,479	$381	$104.8	-0.42%
Search Engines	51913a	$21.51	$7.5	35%	14,577	$1,476	$32.6	8.59%
Database & Directory Publishing in the US	51114	$13.00	$4.5	35%	38,581	$337	$11.6	-1.79%
Electronic & Computer Repair Services	81121	$21.07	$7.05	33%	153,880	$137	$21.17	0.08%
Communication Equipment Manufacturing	33422	$32.37	$10.67	33%	89,822	$360	$35.3	1.51%
Wireless Telecommunications	51332	$229.41	$64.0	28%	277,786	$826	$268.5	2.84%

Industry Segment	IBIS number	2013 Revenues (billions)	2013 Industry Value Added (billions)	% VALUE ADDED	Employees	Revenues per employee (thousands)	2019 Projected Revenue	CAGR
Carriers								
Telecommunications Resellers	51791a	$10.11	$2.7	27%	25,370	$398	$7.9	-3.60%
Telecommunication Networking Equipment Manufacturing	33421	$9.94	$2.51	25%	16,826	$591	$11.65	2.88%
VOIP	51711e	$2.93	$0.7	25%	4,310	$680	$3.8	4.80%
Computer Peripheral Manufacturing	33411b	$22.41	$5.38	24%	44,576	$503	$28.26	4.35%
Satellite TV Providers in the US	51711b	$39.80	$9.3	23%	29,315	$1,358	$44.7	2.05%
Cable Networks in the US	51321	$56.40	$12.9	23%	51,849	$1,087	$59.9	1.03%
Computer Stores	44312	$25.07	$4.80	19%	98,258	$255	$24.15	-0.61%
Wire & Cable Manufacturing	33592	$17.60	$3.10	18%	31,525	$558	$20.17	2.43%
Computer Manufacturing	33411a	$15.04	$2.23	15%	10,626	$1,415	$11.86	-3.53%
Computer & Packaged Software Wholesaling	42343	$351.54	$39.88	11%	314,266	$1,119	$411.07	2.82%
TOTALS		$1,754.24	$605.46	35%	4,621,933	$379.55	$2,036.7	2.68%

Appendix B. Additional Essays

Social Media

Discussion

From the telegraph, to letter delivery, to the telephone, to email, the only thing constant about society's communications method is that it always changes. Just as most people got comfortable with email and cellular telephone calls, the dynamics have changed again with communicating through the social media enterprise as the latest trend. This includes status updates through Facebook, 140-character thoughts via Twitter, latest photos uploaded via Vine and SnapChat, or simple text messages via iMessage, SMS messaging, or Instagram. Outside of the fact that over a billion people are using social media today, the two major trends most impacted by social media are rapid growth in advertising revenues and the impact social media has on the globalization of communication.

Google pioneered the online advertising market more than 10 years ago and has owned huge market share. In 2013, Google owned 33% of the world's $117B in digital ad spending while Facebook, Yahoo, and Microsoft are all under 5%.[128] However, as other companies saw the amount of advertising revenue pouring into Google's targeted advertising capabilities, other social media sites fought to gain market share like Facebook, Twitter, SnapChat, Vine, Pinterest, and gaming apps (like Candy Crush, Flappy Bird). Any tool or application that garnered massive consumer interest immediately caught the eye of online advertisers. In the social media business, active subscribers/users translates into cash value in selling advertising space to companies. Nothing highlights this trend more than the $19B acquisition of WhatsApp by Facebook given WhatsApp's 450M monthly subscribers, translating to about $40/user valuation. This blockbuster deal makes the Facebook $3B offer to SnapChat seem like pocket change that warranted a rejection by the startup photo-sharing application. With the world's population over 7B people, social media companies are hedging their businesses on growing their subscribers even more as more of the world comes online. We have yet to see the peak of social media and the online advertising market.

The other major trend, global communications capability, is more relevant to the Department of Defense (DoD). The freedom to communicate freely across international boundaries has brought people from various backgrounds and interests closer together than ever before. All of a sudden, the ability to mass communicate, share thoughts, voice protests, and share news to millions of people instantaneously is changing the world dynamics. Within minutes of the Washington Navy Yard shooting in September 2013, hundreds of Tweets from people on lockdown, the news media, and even government agencies filled the Internet. In this example, social media was used to keep people updated on breaking news, helped first responders get an idea of the number and status of possible shooters, and notified employees to stay in lockdown. Social media is credited with much of the success in getting the Arab Spring off the ground by linking thousands of activists together for a common cause.[129] Even a simple picture from an event could make social media history. Oscar host, Ellen DeGeneres, set the Twitter records for most retweeted message of all time by snapping a selfie with some of Hollywood's most famous people. The picture broke the record of 1.3M retweets in just 34 minutes.[130] The point is that social media can strike a large audience, in a short amount of time, across international borders like never before.

National Security Implications.

Social media is not just for teenagers and the younger generation. All the trends that highlight the positive impact of social media also cause some important threats to national security.

Terrorists, nation-states, and other potential adversaries have learned how to use the various social media tools to benefit them. For some adversaries, social media is the method to recruit, train, and communicate with their members. For others, social media provides the ability to spread negative propaganda against the U.S. and our allies. Adversaries use tools like YouTube to teach bomb-making skills and suicide vest design while also using it to post videos from successful attacks. A good example of adversaries exploiting social media is the al Qaida-linked Somali insurgent group, al-Shabab, using Twitter to rationalize their actions during a Nairobi mall attack in September 2013.[131] The insurgent group was able to spin the attack as retribution for the perceived injustices against them. They also used Twitter to exaggerate the number of people killed, which was nearly double the actual death toll. Essentially, social media has opened up a new vector for adversaries to launch an attack.

As most would agree, the health of the nation's economy is directly related to national security. A thriving social media industry, like we experience today, creates a positive impact on our nations' economy, which strengthens our national security. While all indications point to continued success of the social media industry, we cannot take it for granted. The implications of the NSA surveillance programs by Edward Snowden could jeopardize the success of the social media industry. The Snowden leaks give rise to serious concerns, both domestically and internationally, over privacy. If consumers turn to foreign alternatives for their social media needs out of concern for how their privacy is treated within the U.S., our social media industry could face a bleaker future.

While the U.S. was already preparing to fight in air, land, sea, space, and cyberspace, adding social media to the cyberspace domain only makes national defense even harder. Social media has opened up a new attack vector for our adversary, and for our country. Social media can be a powerful tool for the DoD and intelligence agencies to gather intelligence, infiltrate adversary sites, and set the conditions for future success of operations. We must defend ourselves from the advantages our adversaries can gain through social media and be prepared to use social media for our own gain.

Recommendations.

While it might not seem obvious at first, the social media industry has a surprisingly strong impact on U.S. national security both in terms of its growing impact on the economy and its applicability to national defense. With over 1.5B subscribers and billions of dollars of revenue generated by the industry, the government must engage with social media smartly. Interfering with restrictive policies will not be accepted, but the country does expect its government to protect the people, even if the people are not protecting themselves.

Policy Recommendations. The only policies that the American people would accept would be ones that increase protection of privacy and personal information. The government should continue with strong privacy regulations that control how companies collect, use, and sell our personal information. Adding teeth to these strong government privacy policies would make companies better protect the information they are entrusted with. This can be done with substantial fines proportional to the revenues of the company (higher fines for more profitable companies). Additionally, harsh criminal penalties imposed on those that commit privacy violations may help deter illegal behavior.

One additional policy the government must institute is transparency on how it collects and uses personal data, not just to benefit social media, but to also improve national and international trust. The American population is smart enough to understand that data collection is necessary to protect national security. However, indiscriminate data collection should be tailored to the minimum amount required to accomplish national security objectives. More importantly, the government must be upfront with what it collects and how it is used.

DoD Recommendations. Knowing that U.S. adversaries are active users of social media, the obvious consequence is that DoD must embrace, protect, and exploit social media as well. First, the U.S. must defend within social media. This includes some degree of protecting individual privacy, stopping illegal or detrimental use of social media like Twitter deleting the account of the Mumbai mall attack jihadists within 24 hours, and monitoring what information is traversing the social media threads. DoD should continue to expand its use of social media to communicate to its stakeholders, recruit its future employees, and exploit its adversary.

Overall Recommendation for Industry. The social media market is still relatively new in the U.S. and abroad. Crazy ridiculous growth over the past 5-10 years has spurred great competition that has been profitable and beneficial for advertisers and consumers, as well as serving as a new medium for national security. At this time, the best thing for our national security, our economy and the industry is to allow it to thrive under normal market conditions with only limited government policy interference but active government participation in social media.

ICT Acquisition

Discussion.

Information technology capabilities are maturing much quicker than the government can incorporate them into weapon systems. The government serial process of research, development, testing, and procurement can take years to complete, compared to an industry process of days or months. Therefore, the government routinely delivers equipment that contains outdated and obsolete components. A more detailed and focused analysis of the DoD ICT acquisition and governance system lends itself to several observations and recommendations that could benefit system procurement and deployment.

Issue #1 – Product modernization and testing.

Our Defense Acquisition System (DAS) is geared heavily toward the serial process of new system requirements and development. However, in several instances a less expensive technology refresh, for an existing and fielded ICT system, would meet the requirement. This is easily done through a continuous cycle of funding allocated for modernization efforts. Equally important, operational and developmental testing procedures need to facilitate the adoption of new technologies and embrace a test-fix-test cycle that can produce qualified upgrades in two years or less.

Issue #2 – Maximize use of COTs products.

The user community routinely begins with generic ICT requirements, but then quickly modifies them toward increasingly difficult and sometimes impossible metrics. This requirements growth trend leads to military unique and development intensive efforts that neglect to consider the resources required, design timeline, and investment for maturity growth. The DoD will then spend an inordinate amount of time trying to pursue those fringe capabilities that often provide very minimal operational benefit. User representatives should instead work with the appropriate program management team, industry members, and test community to explore existing ICT capabilities and work toward improvements through technology insertion over time.

Issue #3 – Spectrum Limitations.

Spectrum is a finite resource and the radio frequency bands are reaching historic global levels of saturation. Coupled with political pressures to return military spectrum for commercial use and the dramatic increase in wireless devices, Industry and DoD must collectively work to advance technologies and concepts. In addition, the U.S. Department of State must continually engage, with DoD and Department of Commerce (DoC) in support, on global spectrum governance activities to protect U.S. national security frequency needs. The DoD Chief Information Officer (CIO) must vigorously pursue policies and direct research investments in these areas. There are compression schemas, multiplexing, and spectrum agility approaches that can greatly enhance our expeditionary, mobility, and geographic spectral freedoms.

Issue #3 – Lowest Price and Technically Acceptable.

Industry consistently states that the government preferred approach for working with industry is for awarding contracts centered on obtaining a Lowest Price Technically Acceptable (LPTA) approach. This has created friction with industry and generated unintended consequences of cheap products and services. A revision of Better Buying Power (BBP) policies must reinforce that the Government desires best value, even if an increased short-term investment is necessary to obtain larger and longer-term savings.

Discussion. DoD guidance to acquisition professionals to apply the LPTA contract structure wherever possible has resulted in missed opportunities and inferior products and services in the ICT area. High quality vendors (in terms of capability and technology) have been pushed aside for low-cost proposals where quality, completeness of solution, and timeliness of delivery often turn out to be problematic. Contractual remedies are costly both in time and money, to the detriment of long-term DoD interests. Acquisition professionals are caught between developing specifications that weed out the riskier vendors and still allow for flexibility and innovation.

From an industry standpoint, LPTA drives business decisions about whether to respond to DoD requests for proposals and ultimately about whether to stay involved in government work at all. Industry technical leaders with the greatest expertise in high demand skills, such as big data, mobile, social, IoE, and intelligent systems, can make the choice to focus on commercial customers and avoid the expense of DoD acquisition processes in situations where they believe they cannot differentiate themselves because of the restricted nature forced by the LPTA selection criteria.

From a DoD perspective, the impact is to “make do” with less innovative vendors who may not have the depth or quality of expertise that is really needed. In later phases, this can result in contractual wrangling, work delays, botched implementations and solutions that do not take advantage of rapid advances in technology. These issues can cause programs to become far more costly than originally envisioned and do a disservice to the warfighter. In an effort to be fair and get the best price, DoD is finding itself suffering from a decline to the lowest common denominator in products and services because of over-reliance on LPTA contracts.

Despite great effort taken by the acquisition community to avert them, vendor protests have become routine for ICT. There is little risk to the vendors and high upside potential for competitors to overturn an award. Use of LPTA contracts means that if a vendor is selected based on better compliance with the requirements, but does not have the lowest bid, competitors will immediately use this as an excuse to protest. Conversely, if the lowest bid is awarded, other competitors can make the claim that the bidder was not as well aligned with the requirements, which was why they could provide a lower price. Sorting protests out for every contract is immensely costly and time-consuming, providing little added value.

Recommendations.

To ensure our acquisition system can meet future consumer demands, the USG should pursue the following policy recommendations.

- Ensure the acquisition and funding process incentivizes modernization and pre-planned improvements for information and communications equipment.
- Align requirements development with an approach to better leverage and procure commercial technologies.
- Pursue more technologies that support the employment of spectrum efficient and agile systems.
- Reinforce the use of best value contracts and not simply lowest price.

Internet of Everything (IoE)

Discussion.

The IoE consists of a large network, devices, and applications that are part of an "ecosystem of connected devices with sensors and intelligence built into physical objects"[132] such as clothing, appliances, transportation systems, and the like. McKinsey defines the IoE as "sensors, actuators, and data communications technology built into physical objects—from roadways to pacemakers—that enable those objects to be tracked, coordinated, or controlled across a data network or the Internet."[133] Two terms are used to describe the activities associated with this industry -- intent of things, and the IoE. The key idea in these definitions is that everyday articles become self-aware via some level of built in processing, and communicate with elements of the wider world via extremely low power networked radios that are interconnected by an expanded wired and wireless Internet backbone.

For the foreseeable future, the IoE will depend on a set of interoperable technologies. The IoE requires a network "skin" that blankets the places people will be. The difficulty is the engineering and design at low cost the low power devices at the user edge. The network "skin" that connects the IoE aware devices must be able to seamlessly switch between the available wireless and wired systems. The network "skin" must seamlessly integrate among global networks. There must be a realization of absolute privacy that includes encryption and obscuration technology for data in motion, data at rest, data in processing, and data in collection. This includes finding a technology that allows the smallest device at the edge to be unbreakable. The IoE must become a platform with open system application programming interfaces (APIs) that allow other developers to build additional services and products on top of the individual devices. The ideas and capabilities behind IoE mean that eventually almost every product will contain some level of IoE capabilities. In this world, competing standards and interfaces will work against the IoE capabilities providing their full capabilities to users

National Security Implications.

The privacy needs of IoE users will need to be balanced against the needs of the national security needs. However, if national security needs mean that the global markets do not trust, and therefore purchase, U.S. IoE devices, the national security system must accept that the IoE must be made unbreakable by any cyber agency.

Recommendations

The U.S. ability to continue to lead the IoE revolution, the USG should adopt a deliberate policy with legal standing that IoE devices will be off limits to all national security intercept except as authorized by a search warrant. The USG identify as a public good the need for a U.S. IoE skin, and direct via an "Highway Construction Act; National Interstate and Defense Highways Act" like law that creates a U.S. IoE skin. The USG works through international agencies to create extensions of this skin in all global markets. The USG establish a national resources that creates unbreakable device, network skin, and processing center standards and then supervise their deployment.

Cloud Computing

Discussion.

Cloud computing will dominate the future of the Information and Technology (IT) industry within the U.S. and globally, having a variety of strategic implications on both the U.S. national security establishment and governments around the world. In North America, 80 percent of businesses are either looking at cloud computing or already have it. The cloud computing market is on its way to generating $100 billion per year.[134] As the chief executive officer of a start-up company specializing in data analytics software says, "Things are downright Darwinian right now. There hasn't been this type of Cambrian explosion in corporate technology in 20 years."[135] These trends will have a tremendous impact on U.S. national security as government leaders and the workforce adapt to this new technology and leverage the power of the cloud. It will be a force multiplier by creating financial and other type of efficiencies and the ability to leverage information to solve national security problems. At the same time, U.S. leadership and security professionals will have to wrestle with security issues brought about by this cloud technology. As this new technology, with its ambiguous border evolves across the globe, the U.S. and other governments will also wrestle with a host of other issues to include: privacy, intellectual property issues, and Internet freedom.

Industry is moving towards cloud computing solutions because of the appeal to save money. With technology constantly evolving, businesses have been through decades of frequent transitions, which have resulted in the input of new software and hardware onto the old systems. Many corporate ICT offices have to spend approximately 70 percent of their funds just to keep everything running, while only 30 percent of their money is spent on exploring new ideas. They often have to invest in huge amounts of equipment to meet increased demands during crisis time and then at other times, this extra equipment sits idle. Companies are struggling to deal with these challenges while also being inundated with so much constant data as a result of the information age. Cloud computing seems to offer solutions for increasing efficiency while decreasing overall costs.[136] For example, during a visit to a U.S. cloud computing provider, one official noted they had seen savings of up to 60% when transferring customers to cloud technology. [137]

Security and privacy are the leading concerns as we become more dependent on cloud computing technology. There is a need for more strategic thinking on these issues as the cloud continues to be a driving factor in the future of information technology. The very notion of turning over important data to another company creates anxiety for some people. Business executives might not take advantage of cloud computing system since they may feel they will not be able to keep the company's information under lock and key.[138] In contrast to that line of thought, companies that are providing such services live and die by their reputations. It would only serve them to incorporate good security service because otherwise they would lose clients and market share. It is very much in the interest of cloud computing companies to protect client data with the most sophisticated techniques.[139] Cloud security also need to be focused on the issue of risk especially since cloud technology creates a potential opportunity for hackers and governments around the world to access data in the cloud.[140] During one Information and Communications Technology Study visit, an official involved with implementing cloud systems within the USG noted that cloud technology was not originally developed with security in mind. He explained they were reverse engineering the cloud technology to ensure it met high-security standards within certain U.S government agencies. Furthermore, he noted many USG leaders seemed unable to manage all the various complexities of the cloud.[141]

Many questions surrounding cloud computing are philosophical and are still being debated in the U.S. and around the world. For example, does a user or the company subscribing to the cloud computing service own the data? The cloud computing system provides the storage, so do they own the data? Could a cloud computing company deny access to data? These are the types of issues that are currently being considered. [142]As well, what if a cloud computing company went out of business suddenly? Where would the data go? Apple's co-founder, Steve Wozniak, is very worried about intellectual property issues and who owns the data. For example, consider the controversy over photos and the changing terms of services for companies like Instagram and Facebook, which are cloud services. Ownership is huge issue of concern.[143] Right now, no central body exists to govern the use of the cloud for storage and services. The Institute of Electrical and Electronics Engineers (IEEE) recently created an IEEE Cloud Computing Initiative in 2011 to establish standards for use, especially for the business sector; however, cloud-computing is a little bit like the old Wild West, where rules are being made up on the fly.[144]

Large and efficient data centers make up the backbone of the global Internet. Continued improvement of hardware and processing/storage capabilities has created innovative Internet services that are available worldwide. This model that was built on market incentives is under scrutiny more and more and governments are viewing data more strategically. They are looking at policies to demand data be stored and processed in-country. The objectives of such policies are diverse and governments believe they can: protect privacy and security of users on the Internet and businesses; enforce local consumer protections; grow local ICT industries; or increase control over content**.**

Snowden revelations are increasing these types of trends. Governments are increasingly under more pressure to do something to protect their Internet users and businesses against surveillance. However, these revelations also give them the cover to further their objectives. Governments are not focusing on the potential of the global network. These types of policies will only make the Internet more expensive and less useful to developing countries and small businesses globally.[145]

National Security Implications.

There are several key national security implications as the USG moves forward with cloud technology implementation. The U.S. leadership and security professionals will have to wrestle with security issues brought about by this cloud technology. Cloud technology could help ease the burden of searching for key information and provide better intelligence and be helpful in trying to predict future issues of concern to U.S. national security. The technology also has the potential to create efficiencies and save money during a critical time of declining budgets.

Recommendations.

Cloud computing has the potential to revolutionize the world. As the technology continues to evolve, the United States national security complex must carefully institute practices that gain the benefits of the technology to harness large amounts of data. At the same time, they must ensure information is protected. Cloud technology should not be seen as a CIO problem. Leaders at all levels must have an understanding of the technology. As well, the United States should work with other governments worldwide to ensure Internet access is not hindered, intellectual property rights are protects, and privacy and security issues are properly addressed.

Net Neutrality

Net neutrality is "the principle that says that all content online should be treated equally by Internet service providers (ISP)."[146] The Federal Communications Commission (FCC) recently asked for public input into a new rulemaking effort to regulate the Internet.[147] The process could result in rules that would allow ISPs to offer faster Internet service to content providers willing to pay for it. Ideally, the Internet should be free and equally open to all lawful content providers. However, given the increasing volume of data each day, ISPs are looking for sources of revenue in order to expand their networks.[148] Consumer advocates fear that any fees paid by content providers would ultimately be passed on to consumers.

Internet freedom advocates are concerned that small websites that do not pay ISPs for access to the "fast lane" will eventually be blocked.[149] This could disproportionately impact small businesses, non-profit organizations, and individuals who publish content for free. Likewise, the major Internet content providers are concerned that allowing ISPs to charge for faster service will make it more expensive for them to provide content, while start-ups could find a major barrier to entering the ICT market.[150] Such outcomes could jeopardize the openness of the Internet.

Net neutrality has national security implications as well. Given that DoD leases most of its communications links from ISPs, a move away from net neutrality could result in higher costs to ensure access for DoD's data. The entire USG could, like other consumers and content providers, also see higher costs to access the Internet. Yet, data will continue to grow exponentially and someone—be it content providers, ISPs, consumers, or taxpayers, or some combination—will eventually have to pay to expand the capacity of the Internet backbone. This is an issue that DoD should monitor for its potential budgetary and national security impacts.

Appendix C – Acronyms

CAGR	Compound Annual Growth Rate
CEO	Chief Executive Officer
CIO	Chief Information Officer
COTS	Commercial off the Shelf
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
FISA	Foreign Intelligence Surveillance Act
GDP	Gross Domestic Product
HPC	High Performance Computing
IBM	International Business Machines
IC	Intelligence Community
ICT	Information Communications Technology
IoE	Internet of Everything
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
IT	Information Technology
LPTA	Lowest Price Technically Acceptable
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
NSS	National Security Strategy
R&D	Research and Development
STEM	Science, Technology, Engineering, and Mathematics
USG	United States Government
VOIP	Voice Over Internet Protocol

REFERENCES

[1] President Barack H Obama, *National Security Strategy* (Washington DC: The White House, May 2010), 27.

[2] U.S. Bureau of Economic Analysis, “ICT Value Added,” http://bea.gov/iTable/itable.cfm?reqid=51&step=1#reqid=51&step=51&isuri=1&5101=1&5102=1&5113=ictva&5111=2005&5112=1 (accessed on January 24, 2014).

[3] U.S. Bureau of Economic Analysis, “ICT Real Value Added,” http://bea.gov/iTable/itable.cfm?reqid=51&step=1#reqid=51&step=51&isuri=1&5101=1&5102=10&5113=ictva&5111=2005&5112=1 (accessed on January 24, 2014).

[4] See Appendix A. Existing industry classifications do not allow for precise measurement. For the rest of this paper, the $1.7 trillion calculated in Appendix A will be used for this analysis.

[5] NAICS codes 33422, 33411a, 33411b, 33421, and 33592 respectively.

[6] NAICS codes 51332, 51711c, and 51791a respectively.

[7] NAICS codes 51711d, 51821, and 51913b respectively.

[8] NAICS codes 51821 and 54151, respectively.

[9] *Mergent Online Home Page*, http://www.mergentonline.com.nduezproxy.idm.oclc.org/advancedsearch.php (accessed April 23, 2014).

[10] R. Glenn Hubbard and Anthony Patrick O’Brien, *Economics*, (Boston: Pearson Education, 2013), 432-6, 460-4.

[11] Ibid.

[12] Kelley King, “Hackfests Are at the Heart of Creativity and Collaboration — and Beer Apps”, *treehouse blog*, http://blog.teamtreehouse.com/hackfests-heart-innovation-invention-creativity April 10, 2014.

[13] Interview with industry source, ICT field visit, February 10, 2014, Washington, DC.

[14] Sarah Kahn, “IBISWorld Industry Report, 33421, Telecommunication Networking Equipment Manufacturing in the US,” January 2014, “http://clients1.ibisworld.com.nduezproxy.idm.oclc.org/reports/us/industry/default.aspx?entid=745, May 1, 2014, 9.

[15] Ibid., 4.

[16] “Yahoo Finance, Sprint Income Statement”, *YAHOO Finance*, http://finance.yahoo.com/q/is?s=S+Income+Statement&annual December 31, 2013.

[17] “Mobile and Cloud Applications”, 2014, http://shop.sprint.com/mysprint/shop/solution/landing_page.jsp?pageId=ecomm_biz_landing_mobility_clouds_landing&INTCID=TSC:BHP:110611:Biz:Need:MobileApps&adSelectData=1:Module_BizNeed_110611 (accessed May 12, 2014).

[18] Scott Sloat, “Sprint and SoftBank Announce Completion of Merger,” *Sprint Newsroom*, http://newsroom.sprint.com/news-releases/sprint-and-softbank-announce-completion-of-merger.htm, July 10, 2013.

[19] Ibid.

[20] Sarah Kahn, "IBISWorld Industry Report, 51332, Wireless Communications Carriers in the US," April 2014, http://clients1.ibisworld.com.nduezproxy.idm.oclc.org/reports/us/industry/default.aspx?entid=1267, May 1, 2014), 10.

[21] Stephen Hoopes, "IBISWorld Industry Report, 51121b, Database, Storage & Backup Software Publishing in the US," March 2014, http://clients1.ibisworld.com.nduezproxy.idm.oclc.org/reports/us/industry/default.aspx?entid=1987, May 1, 2014, 9.

[22] Ibid.

[23] "Yahoo Finance, Oracle Financial Statements", *YAHOO Finance*, http://finance.yahoo.com/q/is?s=ORCL%2C+&ql=1, February 28,2014.

[24] "Yahoo Finance, Google Financial Statements", *YAHOO Finance,* http://finance.yahoo.com/q/is?s=GOOGL%2C+&ql=1, December 31, 2013.

[25] Ibid.

[26] Interview with industry source, April 9, 2014, ICT field visit, Mountain View, CA.

[27] Michael Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors* (New York: Free Press, 1980) http://books.google.com/books?hl=en&lr=&id=QN0kyeHXtJMC&oi=fnd&pg=PR9&dq=michael+porter+strategy&ots=jpHYQmB0Bi&sig=zWmpdTO4eCy2dfxPZ-iKfUc4SAw#v=onepage&q=michael%20porter%20strategy&f=false (accessed May 12, 2014).

[28] "IBM's A Software Company Now!", *BusinessInsider*, http://www.businessinsider.com/ibm-software-company-2012-8 (accessed May 16, 2014).

[29]Nathan Myhrvold, "The Big Idea: Funding Eureka!", *Harvard Business Review*, http://hbr.org/2010/03/the-big-idea-funding-eureka/ar/1 (accessed May 16, 2014).

[30] M. E. Porter, "What is a strategy*?" Management and Accounting Web,* http://maaw.info/ArticleSummaries/ArtSumPorter96.htm (accessed May 15, 2014).

[31] "Strategic Positioning", *Dean and Company*, http://www.dean.com/delta-model/strategic-positioning (accessed May 15, 2014).

[32] Ibid.

[33] "About Google," *Google*, http://www.google.com/about/ (accessed May 16, 2014).

[34] "Strategic Positioning," *Dean and Company*, http://www.dean.com/delta-model/strategic-positioning (accessed May 15, 2014).

[35] Henry Blodget, "Apple's 'Mission Statement' Is Making People Worry That The Company Has Gone To Hell," *Business Insider*, http://www.businessinsider.com/apples-new-mission-statement-2013-8 (accessed May 16, 2014).

[36] "Strategic Positioning," *Dean and Company*, http://www.dean.com/delta-model/strategic-positioning (accessed May 15, 2014).

[37] "Form 10-K Oracle Corporation," *Oracle,* http://www.oracle.com/us/corporate/investor-relations/financials/10k-fy2013-2021362.pdf (accessed May 16, 2014).

[38] "Strategic Positioning," *Dean and Company*, http://www.dean.com/delta-model/strategic-positioning (accessed May 15, 2014).

[39] "Www.Companiesandmarkets.Com: IT Services in China." *M2 Presswire,* http://search.proquest.com.nduezproxy.idm.oclc.org/docview/444280020?accountid=12686, April 28, 2009.

[40] "Request for Public Comments regarding the National Trade Estimate Report on Foreign Trade Barriers. 2013," *Lanham: Federal Information & News Dispatch, Inc*., http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1426123010?accountid=12686.

[41] Henry Blodget, "This Article Explains Why Apple Makes iPhones In China And Why The U.S. Is Screwed", *Business Insider*, http://www.businessinsider.com/you-simply-must-read-this-article-that-explains-why-apple-makes-iphones-in-china-and-why-the-us-is-screwed-2012-1 (accessed May 16, 2014).

[42] "Www.Companiesandmarkets.Com: IT Services in China." *M2 Presswire,* http://search.proquest.com.nduezproxy.idm.oclc.org/docview/444280020?accountid=12686, April 28, 2009.

[43] "Request for Public Comments regarding the National Trade Estimate Report on Foreign Trade Barriers. 2013," *Lanham: Federal Information & News Dispatch, Inc*., http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1426123010?accountid=12686.

[44] Michael Minges, et. al., "Information and Communications in the Chinese Countryside," *The World Bank*, 2014, http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/04/28/000333037_20140428124209/Rendered/PDF/876000PUB0978100Box382175B00PUBLIC0.pdf, April 29, 2014.

[45] U.S. Congress, House, Permanent Select Committee on Intelligence, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 112th Congress, 2nd sess., October 8, 2012. In 2012, Congress publicly determined that the USG should not purchase equipment from Huawei because of fears that the People's Liberation Army (PLA) had built secret backdoors into Huawei's hardware that could be used to gain illicit access to data. Other countries followed the US's lead in shunning Huawei even though its products were much less expensive than similar US products.

[46] Joel Snyder, "The Huawei Security Risk: Factors to Consider Before Buying Chinese IT," *TechTarget*, http://searchsecurity.techtarget.com/feature/The-Huawei-security-risk-Factors-to-consider-before-buying-Chinese-IT, May 1, 2014.

[47] Eric Zeman, "Huawei Becomes Third Largest Smartphone Maker," *Information Week*, http://www.informationweek.com/mobile/mobile-devices/huawei-becomes-third-largest-smartphone-maker/d/d-id/1108354?, January 25, 2013.

[48] Michael S. Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment," *New York Times*, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html?pagewanted=all&_r=0, October 8, 2012.

[49] Schmidt, “U.S. Panel Cites Risks.”

[50] Sinha, Paresha, Michèle E.M. Akoorie, Qiang Ding, and Qian Wu. "What Motivates Manufacturing SMEs to Outsource Offshore in China?" *Strategic Outsourcing: An International Journal* 4, no. 1 (2011): 67-88. doi:http://dx.doi.org/10.1108/17538291111108435. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/855079797?accountid=12686.

[51] Mohiuddin, Muhammad, PhD. and Zhan Su PhD. "Manufacturing Small and Medium Size Enterprise's Offshore Outsourcing and Competitive Advantage: An Exploratory Study on Canadian Offshoring Manufacturing SMEs." *Journal of Applied Business Research* 29, no. 4 (Jul, 2013): 1111-1130. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1413874159?accountid=12686.

[52] Interview with industry sources (multiple), April 7-11, California

[53] Interview with industry source, April 8, 2014, industry visit, San Jose, CA.

[54] Interview with industry source, April 8, 2014, industry visit, San Jose, CA.

[55] Daniel Eran Dilger, “Apple's iPhone Takes 80 Percent of China's Booming Premium Phone Market,” *appleinsider*, http://appleinsider.com/articles/14/03/14/apple-inc-iphone-takes-80-percent-of-chinas-booming-premium-phone-market-aapl, March 14, 2014.

[56] Paul R. LaMonica, “Baidu: Is China's Google Better than Google?” *CNN Money*, http://money.cnn.com/2012/02/13/technology/thebuzz/, February 13, 2012.

[57] Table A.1, Appendix A this paper.

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] "Reshoring manufacturing: Coming home”, *The Economist*, http://www.economist.com/news/special-report/21569570-growing-number-american-companies-are-moving-their-manufacturing-back-united, January 19, 2013.

[62] Josh Timberlake, “Manufacturing beyond China: New Options. New Opportunities, New Risks”, *Deloitte University Press*, http://dupress.com/articles/manufacturing-beyond-china, May 16, 2014.

[63] William H. Lehr1, John M. Chapin. “On the Convergence of Wired and Wireless Access Network Architectures”, *Business Innovation*, http://businessinnovation.berkeley.edu/Mobile_Impact/Lehr_Chapin_IEP.pdf, May 16, 2014.

[64] Mirren Gidda, "Edward Snowden and the NSA files – timeline," *The Guardian*, http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, July 25, 2013.

[65] Interview with an industry source, ICT Industry Study visits conducted in Silicon Valley, California from 6-10 April 2014.

[66] *U.S. National Security Strategy*, (2010), *www.whitehouse.gov*, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, 17.

[67] Robert S. Litt, "Privacy, Technology & National Security: An Overview of Intelligence Collection," *IC on the Record*, July 18, 2013, 1, http://icontherecord.tumblr.com/post/57724442606/privacy-technology-national-security-an (accessed March 30, 2014). According to Mr. Litt, Snowden's disclosures "threaten to cause long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our Nation. And because these disclosures were made by people who did not fully understand what they were talking about, they were sensationalized and led to mistaken and misleading impressions." Ibid. See also Director of National Intelligence, "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," June 8, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act (accessed April 30, 2014).

[68] Robert S. Litt, "Privacy, Technology & National Security: An Overview of Intelligence Collection," *ODNI General Counsel*, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection, July 18, 2013, 9.

[69] Charlie Savage, "Obama to Call for End to N.S.A.'s Bulk Data Collection," *The New York Times*, http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=0, March 24, 2014. Uncollected metadata would remain in the hands of the ICT providers as normal business records under their normal storage and disposal policies.

[70] 50 USC §§ 1801-1885c (2014). Gidda, "Edward Snowden and the NSA Files—timeline," Ibid., 5.

[71] Two commissions reviewed the telephony metadata collection program and the PRISM program. The President's Review Group on Intelligence and Communications Technologies issued its report on December 12, 2013. The report is available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed March 30, 2014). The President also directed a new federal agency, the Privacy and Civil Liberties Oversight Board, to conduct a similar review. The PCLOB issued part 1 of the report on the telephony metadata and operations of the FISC on January 23, 2014. The report is available at http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf (accessed April 30, 2014). The PCLOB expects to issue a second report on the PRISM program in Spring 2014.

[72] Craig Timberg and Jia Lynn Yang, "Google is encrypting search globally. That's bad for the NSA and China's censors," *The Washington Post*, http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china/, March 12, 2014.

[73] Claire Cain Miller, "Revelations of N.S.A. Spying Cost U.S. Tech Companies," *The New York Times*, March 21, 2014, 1, 4, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (accessed March 29, 2014).

[74] Ibid., 2.

[75] Ibid.

[76] Ibid., 3.

[77] Interview with industry source, ICT Industry Study visits conducted in Silicon Valley, California from 6-10 April 2014.

[78] Interview with industry source, ICT Industry Study visits conducted from 13-18 April 2014 in Shenzhen and Beijing, China.

[79] Cade Metz, "Google Reinvents How Cloud Computing Is Priced", *Wired*, http://www.wired.com/wiredenterprise/2014/03/google-cloud-prices/, March 25, 2014.

[80] One example is National Security Agency Public Affairs Office, "Statement in Response to Press Allegations, March 13, 2014, http://www.nsa.gov/public_info/_files/speeches_testimonies/2014_03_14_press_allegations_response.pdf (accessed March 30, 2014). The press release states only:

Recent media reports that allege NSA has infected millions of computers around the world with malware, and that NSA is impersonating U.S. social media or other websites, are inaccurate. NSA uses its technical capabilities only to support lawful and appropriate foreign intelligence operations, all of which must be carried out in strict accordance with its authorities. Technical capability must be understood within the legal, policy, and operational context within which the capability must be employed.

NSA's authorities require that its foreign intelligence operations support valid national security requirements, protect the legitimate privacy interests of all persons, and be as tailored as feasible. NSA does not use its technical capabilities to impersonate U.S. company websites. Nor does NSA target any user of global Internet services without appropriate legal authority. Reports of indiscriminate computer exploitation operations are simply false.

[81] *Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 126-127. According to the group, "Another dimension to the secrecy vs. transparency issue concerns the role of whistle-blowers. Although an individual government employee or contractor should not take it upon himself to decide on his own to 'leak' classified information because he thinks it would be better for the nation for the information to be disclosed, it is also the case that a free and democratic nation needs safe, reliable, and fair-minded processes to enable such individuals to present their concerns to responsible and independent officials. After all, their concerns might be justified. It does not serve the nation for our government to prevent information that should be disclosed from being disclosed. Although such mechanisms exist, they can certainly be strengthened and made more accessible."

[82] Robert S. Litt, "Privacy, Technology & National Security: An Overview of Intelligence Collection," *ODNI General Counsel*, http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection , July 18, 2013, 9.

[83] Barack H. Obama, "Presidential Policy Directive 28/PPD-28, Signals Intelligence Activities" (Washington, DC: The White House, January 17, 2014).

[84] "U.S. Federal Cybersecurity Market Forecast 2013-2018," *Market Research Media*, http://www.marketresearchmedia.com/?p=206, 30 March 2014.

[85] “Public Good”, *Investopedia*, http://www.investopedia.com/terms/p/public-good.asp (accessed May 16, 2014).

[86] Eric Weiss, and Rena S. Miller, “The Target Data Breach: Frequently Asked, Questions”, *Federation of Atomic Scientists*, http://www.fas.org/sgp/crs/misc/R43496.pdf, April 22, 2014.

[87] “Framework for Improving Critical Infrastructure Cybersecurity,” *National Institute for Standards and Technology*, http://www.nist.gov/cyberframework/, February 12, 2014.

[88] David Schilling, “U.S. Spending $75 Billion A Year Fighting Cyber Threats And Attacks,” *Industry Tap Into News*, http://www.industrytap.com/us-spending-75-billion-a-year-fighting-cyber-threats-and-attacks/4699, August 10, 2013.

[89] Valentina Pasquali, “Cover: The Untold Cost of Cybersecurity,” *Global Finance*, http://www.gfmag.com/archives/175-may-2013/12482-cover-growing-threat-the-untold-costs-of-cybersecurity.html#axzz2xSwvZ5gA, 30 March 2014.

[90] The Commission on the Theft of American Intellectual Property, “The IP Commission Report,” May 2013, 2, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf (accessed on 30 March 2014).

[91] “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013-2018, *CISCO White Paper*, http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html#~forecast (accessed May 16, 2014).

[92] “Report To The President, Realizing The Full Potential Of Government-Held Spectrum To Spur Economic Growth,” *www.whitehouse.gov*, http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf, July 2012.

[93] Brian Chen, “Mobile Carriers Warn of Spectrum Crisis”, *New York Times*, http://www.nytimes.com/2012/04/18/technology/mobile-carriers-warn-of-spectrum-crisis-others-see-hyperbole.html?pagewanted=all&_r=0, April 17, 2012.

[94] Kelsey Sheehy, "Colleges Fight to Retain Interest of STEM Majors," *Yahoo News*, http://news.yahoo.com/colleges-fight-retain-interest-stem-majors-164159878.html;_ylt=A0LEVxmBrnRTJUMASU5XNyoA;_ylu=X3oDMTEza3AxMXVkBHNlYwNzcgRwb3MDNARjb2xvA2JmMQR2dGlkA1ZJUDQzOF8x, June 19, 2013.

[95] “The STEM Workforce: An Occupational Overview”, *Department for Professional Employees, AFL-CIO*, http://dpeaflcio.org/programs-publications/issue-fact-sheets/the-stem-workforce-an-occupational-overview/, May 15, 2014.

[96] “H1B Cap Reached in First Week: 124,000 H1B Petitions Filed”, *Murthy Law Firm*, http://www.murthy.com/2013/04/08/h1b-cap-reached-in-first-week-124000-h1b-petitions-filed/ April 8, 2013.

[97] Caitlin Dickson, “Obama Administration Proposes New Immigration Rules Without Congress,” *Daily Beast*, http://www.thedailybeast.com/articles/2014/05/06/obama-administration-proposes-new-immigration-rules-without-congress.html, May 16, 2014.

[98] Lisa Rein, “Wave of retirements hitting federal workforce, *Washington Post Politics*, ”http://www.washingtonpost.com/politics/wave-of-retirements-hitting-federal-workforce/2013/08/26/97adacee-09b8-11e3-8974-f97ab3b3c677_story.html, August 26, 2013.

[99] According to the Department of Labor, "The number of new visas that can be issued each year is subject to a cap. H-1B visas are capped at 65,000 during a fiscal year; an additional 20,000 are available to those individuals who received a master’s degree or higher from a U.S. institution of higher education." http://www.dol.gov/compliance/guide/h1b.htm (accessed May 15, 2014).

[100] “How Long an H-1B Worker Can Stay in the United State”, *NOLO Law for All*, http://www.nolo.com/legal-encyclopedia/how-long-h-1b-worker-can-stay-the-united-states.html (accessed May 15, 2014).

[101] Frank J. Ohlhorst, “*Big Data Analytics, Turning Big Data into Big Money*”, John Wiley & Sons, 2013, 2.

[102] “IBM big data and information management”, *IBM Watson Foundataion*, http://www-01.ibm.com/software/data/bigdata/ (accessed May 16, 2014).

[103] Scott Patterson, High Speed Stock Traders Turn to Laser Beams, http://online.wsj.com/news/articles/SB10001424052702303947904579340711424615716 (accessed 16 May 2014)

[104] “IBM big data and information management”, http://www-01.ibm.com/software/data/bigdata/ (accessed May 16, 2014).

[105] *Senate Armed Services Committee Hearing*. Lanham: Federal Information & News Dispatch, Inc, 2014. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1520776430?accountid=12686.

[106] Salvatore Salamone, “Energy Companies Lead in Commercial Supercomputer Adoption”, http://www.energycentral.com/enduse/demandresponse/articles/2863/Energy-Companies-Lead-in-Commercial-Supercomputer-Adoption/, May 16, 2014

[107] "Game on." *The Economist (Online)* (Mar 10, 2014). http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1506536771?accountid=12686.

[108] Mohana Ravindranath, "Global Supercomputer Revenue Down 29 Percent in 2013 (Posted 2014-03-25 20:52:09)." *The Washington Post*, Mar 25, 2014. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1509994801?accountid=12686.

[109] Joel Hruska, “DARPA summons researchers to reinvent computing,” *ExtremeTech*, http://www.extremetech.com/computing/116081-darpa-summons-researchers-to-reinvent-computing, May 16, 2014.

[110] K. Roche, “Supercomputer Brain Simulation”, *IBM.COM*, https://www-304.ibm.com/connections/blogs/stgar/entry/supercomputer_brain_simulation3?lang=en_us (accessed May 16, 2014).

[111] “Department of Defense Fiscal Year (FY) 2013 President's Budget Submission”, *DARPA*, http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id=2147484865 (accessed May 16, 2014).

[112] Frank Konkel, “The intelligence community's big-data problem”, *FCW,* http://fcw.com/articles/2014/03/13/ic-big-data.aspx (accessed May 16, 2014).

[113] National Security Strategy (May 2010), 15.

[114] “Ten Practical Big Data Benefits,” *Data Science Series,* http://datascienceseries.com/stories/ten-practical-big-data-benefits (accessed May 16, 2014).

[115] “Big Data: Benefits, Challenges, and Best Practices”, *tdwi,* http://tdwi.org/Articles/2012/06/26/Big-Data-Best-Practices.aspx?Page=1 (accessed May 16, 2014).

[116] “Gartner Says Worldwide ICT Spending Forecast to Reach $3.7 Trillion in 2013,” *Gartner,* http://www.gartner.com/newsroom/id/2292815 (accessed April 30, 2014).

[117] David Perera, “2014 Budget Request: DoD ICT and DISA”, *FierceGovernmentIT,* http://www.fiercegovernmentit.com/story/2014-budget-request-dod-it-and-disa/2013-05-12 (accessed April 30, 2014).

[118] “Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap”, *DoDCIO,* http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf, (September 2011), 22.

[119] Federal Acquisition Regulation, Part 15.101-2, http://acquisition.gov/far/current/html/Subpart%2015_1.html (accessed May 26, 2014).

[120] Interviews with industry sources, ICT Industry Study visits conducted in Silicon Valley, California from 6-10 April 2014.

[121] “Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology”, *AT&L,* http://www.acq.osd.mil/dsb/reports/ADA498375.pdf (accessed May 16, 2014).

[122] A. Xiao-Yan, X. Dong-Sheng, Z. Feng, & D. Jian-Gang. (2013). “Agriculture intelligent control system algorithm for wireless sensor networks based on Internet of things,” *Sensors & Transducers, 158*(11), 70-75, http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1509394740?accountid=12686.

[123] "Health and Happiness; M-Health." *The Economist,* 410, no. 8872 (Feb 01, 2014): 56-57. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/1493830824?accountid=12686.

[124] “Ready for 650% More Data In Five Years”, *CSC*, http://www.csc.com/insights/flxwd/78931--%E2%80%90big_data_universe_beginning_to_explode (accessed May 15, 2014).

[125] “The Internet of Things”, *Cisco*, http://share.cisco.com/Internet-of-things.html (accessed May 16, 2014).

[126] Barack Obama, “Remarks by the President on Securing Our Nation’s Cyber Infrastructure,” *www.whitehouse.gov*, http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed May 16, 2014).

[127] "Press Release." Board of Governors of the Federal Reserve System, http://www.federalreserve.gov/newsevents/press/monetary/20120125c.htm (accessed April 24, 2014).

[128] Amir Efrati, "In Online Ads, There's Google—and Then Everybody Else." *Wall Street Journal Digits Tech News*, http://blogs.wsj.com/digits/2013/06/13/in-online-ads-theres-google-and-then-everybody-else/ (accessed May 9, 2014).

[129] Don Tapscott, "Social Media Can Help Build Arab Governments Too," *Huffington Post,* http://www.huffingtonpost.com/don-tapscott/egypt-social-media-_b_865862.html, May 23, 2011.

[130] Brad Gerick, "Oscar 2014: Ellen DeGeneres' All-Star Selfie sets Twitter Record." *NY Daily News*, http://www.nydailynews.com/entertainment/oscars/degeneres-all-star-oscar-selfie-sets-twitter-record-article-1.1708566, March 2, 2014.

[131] Will Oremus, "Militant Group Behind Kenya Mall Attack," *Future Tense,* http://www.slate.com/blogs/future_tense/2013/09/21/al_shabaab_on_twitter_hsmpress_tries_to_justify_nairobi_kenya_mall_shooting.html (accessed March 28 2014).

[132] Rakesh Sharma, "A New Perspective on the Internet of Things." *Forbes,* (February 18, 2014).

[133] Manyika, J., M. Chui, J. Bughin, R. Dobbs, and A. Marrs. *Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy,* 2013, 52.

[134] "IDC Predicts 2014 Will Be a Year of Escalation, Consolidation, and Innovation as the Transition to IT's '3rd Platform' Accelerates," *IDC,* http://www.idc.com/getdoc.jsp?containerId=prUS24472713, December 03, 2013.

[135] Ashlee Vance, "The Cloud: Battle of the Tech Titans," *Bloomberg Businessweek Magazine,* http://www.businessweek.com/magazine/content/11_11/b4219052599182.htm, March 03 2011.

[136] Cade Metz, "Google Reinvents How Cloud Computing Is Priced", *Wired,* http://www.wired.com/wiredenterprise/2014/03/google-cloud-prices/, March 25, 2014.

[137] Interview with industry source, ICT field visit, April 10, 2014, Mountain View, CA.

[138] Jonathan Strickland, "How Cloud Computing Works" *www.howstuffworks.com*, http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm (accessed May 16, 2014).

[139] Ibid.

[140] Andrew A. Proia, "Featured Paper: Cloud Computing Security and Privacy" *Cybercrime Review*, http://www.cybercrimereview.com/2013/04/featured-paper-cloud-computing-security.html, April 30, 2013.

[141] Interview with industry source, ICT field visit, April 10, 2014, Mountain View, CA.

[142] Jonathan Strickland, "How Cloud Computing Works" *www.howstuffworks.com*, http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm, May 16, 2014.

[143] Eric Griffith, "What Is Cloud Computing?" *PC Magazine,* http://www.pcmag.com/article2/0,2817,2372163,00.asp, March 13, 2013.

[144] Ibid.

[145] Cade Metz, “Google Reinvents How Cloud Computing Is Priced”, *Wired*, http://www.wired.com/wiredenterprise/2014/03/google-cloud-prices/, March 25, 2014.

[146] Cecelia Kang, "FCC Approves Plan to Consider Paid Priority on Internet," *The Washington Post*, , http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/15/fcc-approves-plan-to-allow-for-paid-priority-on-Internet/?tid=pm_business_pop, May 15, 2014.

[147] FCC, Press Release, "FCC Launches Broad Rulemaking on How Best to Protect and Promote the Open Internet; Seeks Public Input over the Next Four Months to Find Most Viable Approach," May 15, 2014, http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0515/DOC-327104A1.pdf (accessed May 16, 2014). The FCC is taking this step because, in January 2014, a federal appellate court held that the FCC's Open Internet Order, which required strict net neutrality, was mostly invalid because the FCC exceeded its regulatory authority under the Telecommunications Act of 1996. See *Verizon v. FCC*, Case No. 11-1355, decided January, 14, 2014, U.S. Court of Appeals for the District of Columbia Circuit, http://www.cadc.uscourts.gov/Internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf (accessed May 16, 2014).

[148] For example, Netflix traffic alone constitutes over one third of Verizon's U.S. Internet traffic at 8:00pm each night, so it seems fair that Netflix should have to pay more to ensure that its content flows at the speeds necessary for its subscribers to watch video seamlessly. ICT Industry Visit, February 27, 2014.

[149] Cecilia Kang, "FCC Approves Plan to Consider Paid Priority on Internet." *Washington Post*, May 15, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/05/15/fcc-approves-plan-to-allow-for-paid-priority-on-internet/?tid=pm_pop, May 15, 2014.

[150] Ibid.