Spring 2012
Industry Study

Final Report
Information and Communications Technology Industry

<u>The Industrial College of the Armed Forces</u>
National Defense University
Fort McNair, Washington, D.C. 20319-5062

INFORMATION & COMMUNICATIONS TECHNOLOGY INDUSTRY REPORT

ABSTRACT: The Information and Communications Technology (ICT) industry powers productivity gains in the global economy while connecting an ever-increasing number people. While U.S. companies continue to lead the industry, serious challenges place the future of this dominant position in doubt. U.S. comparative advantage is driven by innovation; however, the U.S. government's former position as a technology driver has in many respects regressed to that of an ordinary large consumer of ICT. The U.S government no longer possesses the technical clout or buying power to influence the industry, nor has its policy and regulations kept pace with technology. Its 20th century industrial age bureaucracy is not equipped to lead in this information age sector. Government must first transform its institutions and processes before it can effectively understand and regulate the ICT industry. This report's conclusions were determined by visiting with executives at ICT organizations in Washington, D.C., Silicon Valley, CA, China, and Vietnam, and by referencing relevant literature and media publications in the course of individual research on specific issues.

Lieutenant Colonel Corina Barrow, U.S. Army
Ms. Jenna Ben-Yehuda, Department of State
Ms. Jill Christensen, Defense Intelligence Agency
Lieutenant Colonel Thomas Clancy, U.S. Army
Commander Richard Davis, U.S. Navy
Lieutenant Colonel Charles Ellis, U.S. Marine Corps
Lieutenant Colonel Thomas Falzarano, U.S. Air Force
Mr. Daniel Fri, Department of the Air Force
Captain Anthony Hansen, U.S. Navy
Colonel Stewart Liles, U.S. Army
Mr. D. Scott Martin, Department of the Air Force
Captain Steven McAlearney, U.S. Navy
Lieutenant Colonel Brett Pennington, U.S. Air Force
Colonel Carlos Perez, U.S. Army
Ms. Jody Pugh, Department of Energy
Ms. Roxanna Zamora, Department of the Air Force

Mr. Feza Koprucu, Department of Homeland Security, Faculty Lead
Colonel Richard Altieri, J.D., U.S. Army (Retired), Faculty
Colonel Michael Black, J.D., U.S. Army, Faculty
Colonel Lynne Thompson, EdD, U.S. Air Force (Retired), Faculty

PLACES VISITED

Domestic:
Apple (Cupertino, CA)
AT&T (Washington, DC)
Brocade Communications (San Jose, CA)
Cisco Systems (San Jose, CA)
CSC, North American Public Sector (Reston, VA)
CTIA- The Wireless Association (Washington, DC)
Defense Information Systems Agency (Ft. Meade, MD)
Facebook (Palo Alto, CA)
Google (Mountain View, CA)
IBM (Washington, DC)
Juniper Networks (Sunnyvale, CA)
Microsoft Corporation (Reston, VA)
National Cable Television Association (NCTA) (Washington, DC)
Oracle (Redwood City, CA)
Software and Information Industry Association (SIIA) (Washington, DC)
Sprint (Reston, VA)
TechAmerica (Washington, DC)
Telecommunications Industry Association (TIA) (Washington, DC)
U.S. Cyber Command (Ft. Meade, MD)
Verizon (Reston, VA)

International:
Baidu, Beijing, China
Business Roundtable with BDA, J. Capital Research and USITO, Beijing, China
China Academy of Telecommunications Research (CATR), Beijing, China
Intel, Saigon Hi-Tech Park, Ho Chi Minh City, Vietnam
FPT Telecom, Ho Chi Minh City, Vietnam
FPT Software, Ho Chi Minh City, Vietnam
Huawei, Shenzhen, China
HPT, Ho Chi Minh City, Vietnam
Microsoft, Beijing, China
U.S. Consulate, Hong Kong, China
VNG, Ho Chi Minh City, Vietnam

Chapter 1: Introduction

The Information and Communications Technology (ICT) industry produces the foundational products and services which comprise the cyberspace domain, dramatically impacting all aspects of U.S. national power in the information age. ICT provides a direct contribution to U.S. economic might by enabling efficiencies and productivity gains in nearly every other industry. ICT drives cultural changes in consumers, private firms, governments and international organizations. Within the ICT industry, dynamic innovation is occurring at a dizzying pace. In many respects, this pace of change has outstripped the U.S. government's ability to create relevant policy and regulatory frameworks. Today, the U.S. is at the vanguard of the global transformation from the industrial to the information age. However, while much has already changed, significant innovation and even disruptive change may lay ahead.

Cyberspace challenges our fundamental notions of sovereignty, citizenship, trade, and jurisdiction, which form the very fabric of the Westphalian nation state and the international system of governance. Many industrial age institutions, including U.S. federal, state and local governments, are struggling to adapt. Those more proficient in leveraging information age technologies continue to prosper. However, the growing capability, policy and regulatory gaps between industrial age and information age institutions present significant challenges to U.S. national security and senior policy makers.

The ICT industry has also been a fundamental source of economic growth. The U.S. has been a leader in unleashing this power and maximizing the potential of innovative businesses. The U.S. remains the center of gravity for ICT innovation and growth, but subtle shifts have begun to occur that may reflect a mismatch between an industrial age government and an information age economy. Specific challenges to U.S. national security in the ICT industry include the areas of cyberspace freedom, connectivity, security and competitiveness. Within these areas, several conditions exist which could challenge U.S. dominance.

1. Global conditions that would diminish or drive away current U.S. sources of economic strength and comparative advantage, whether individual or corporate (regulation and corporate tax structures)
2. Global conditions that make the U.S. vulnerable within cyberspace (supply chain security and cybersecurity), including reconciling public-private cybersecurity information-sharing with the realities of global corporate competition and liability
3. Global conditions that jeopardize U.S. comparative advantages in innovation: protection of intellectual property rights, knowledge and learning, research, development, and applied engineering (critical information age economic functions)

The U.S. should enact policies to maximize ICT enabled economic growth and innovation while minimizing burdensome regulations. This requires a disciplined whole of government effort, in concert with industry leaders, to stimulate, invest and regulate the industry. Tempering the voice of powerful lobbying groups and special interests will require research, citizen/policy maker education and candid dialogue. Finally, we must recognize that government now plays a subordinate role in technological development. National security concerns no longer drive technological change in the industry as they once did. The implications of this sea change are dramatic and will shape policy recommendations laid out later in this study.

Chapter II: The Industry Defined

The global ICT industry consists of the firms (U.S., international, and multinational) that provide hardware, software, and services comprising the cyberspace domain. Although not exhaustive, examples of ICT firms include wired/wireless telecommunications providers; networking equipment manufactures; commercial software, application, and operating system developers; cloud service providers; internet portals (Google/ Baidu) and cyberspace security firms. The ICT industry does not include content developers, such as advertising firms, subscription data services, entertainment content (movies, music, or books), or merchants who merely employ cyberspace as a marketplace. With this succinct definition, we turn to examine the condition of the industry.

Chapter III: Current Condition

The ICT industry is healthy. This study used Porter's Five Forces and further examined the current status from the perspectives of economics and policy considerations. Economically, the industry is very healthy and balanced. As mentioned previously, the ICT industry provides hardware, software, and services for all other sectors in economy. Furthermore, the health of the ICT industry is imperative for the health of all other industries and the economy overall. While Porter's Five Forces (Appendix D) shows specific segments of the industry are unique (most specifically in terms of buyer and supplier power), overall the industry provides tremendous economic benefit and greatly enhances U.S. national security. Consistently robust competition and high buyer power have fueled innovation and the need for rapid change. From a policy perspective the landscape is more complicated. Each new ICT innovation has the potential to drive policy changes and increase the complexity of the overall policy landscape. For example, the increase in machine-to-machine communication brings with it a host of privacy and sovereignty concerns. Proper government regulation and involvement is required. However, heavy-handed government policy and misdirected regulations or legislation present the greatest threat to industry health.

Economics: The ICT industry contributes significantly to Gross Domestic Product (GDP). Currently, U.S. GDP stands at about $15 trillion.[1] The magnitude of the ICT contribution to U.S. GDP speaks volumes about the importance of the industry to U.S. economic well-being. According to a recent study, the ICT industry "…contributed about $1 trillion to U.S. GDP, or about 7.1 percent…."[2] The authors attributed approximately $600 billion to "direct contributions" from firms' own operations and approximately $400 billion to "indirect contributions"—benefits to other sectors as a result of using ICT products and services.[3] In terms of direct GDP contributions, we see an increase of almost 25 percent since the early 90s.[4]

It's also insightful to look at the impact in terms of worker productivity. A Federal Reserve economists' analysis, cited in the same study, identified significant gains in productivity in three dimensions: first, the use of ICT technologies directly accounted for 28 percent of U.S. gains in productivity from 1995 to 2001; second, ICT capital investments contributed another 34 percent in gains; finally, changes in organizational structure and training as a result of ICT added another 10 percent.[5] Therefore, when one considers the positive and significant impact of the ICT sector on the economy and worker productivity, decision makers should advocate policies conducive to the further development and growth of this vital industry.

With this in mind, the ICT industry has the potential to stimulate even more economic growth. However, several policy modifications must first be considered. Unfortunately, current U.S. income taxes on corporations are structured in a manner that actually impedes the global competitiveness of the U.S. ICT industry. The U.S. corporate income tax rate is one of the highest in the world and incentivizes global U.S. ICT companies to keep their foreign income overseas. The R&D tax credit is extended by Congress one year at a time, which impedes its effectiveness as an incentive for longer term R&D. According to Shapiro and Mathur, a 10 percent decrease in the corporate tax burden would spur approximately $71 billion of investment in ICT over three to five years.[6] This increased investment in ICT would then generate an additional $450 billion in private-sector spending.[7] Forbes, citing a U.S. Chamber of Commerce report, states that a tax break similar to one passed in 2005 could boost GDP by $360 billion and create 3 million jobs.[8]

One other tax issue of interest is the political discussion regarding an internet sales tax. Currently, an on-line business does not have to collect sales taxes unless it has a "physical presence" in the state of sale.[9] Advocates of internet sales tax state that under the present system, businesses that must collect tax are disadvantaged by the law; taxes are more regressive; and revenue for state and local governments is diminished.[10] Opponents of the measure argue that new taxes on consumers could exacerbate an already weakened economy.[11] Ultimately, although this issue has the potential to significantly impact the ICT industry indirectly, it is fundamentally a consumer tax issue, not a direct ICT economic or national security issue.

Policy: From its infancy, the ICT industry enjoyed limited federal governance. This lack of early governance aided in the rapid expansion of IT and allowed for the free flow of innovation and commercial market development for the internet to become a new household "utility" for the 21st century. This is analogous to electricity or wired telephone services of the last century. Although the "wild west" new frontier approach facilitated rapid innovation and growth of IT and, more specifically, the internet, there comes a point, as it did with electricity and the telephone, that national and state governance must assume a proper but measured role. That time has come. For the betterment of the U.S. economy and national security, a national strategy and appropriate federal and state governing bodies must be put in place for the U.S. to compete in the current global environment. The FCC's National Broadband Plan, electromagnetic spectrum management, and network neutrality efforts, along with Federal and DoD IT governance might be positive steps towards creating the structure required for the industry to thrive.

However, the current environment is complicated by a set of interrelationships that make it difficult to develop adequate policy and appreciate second and third-order effects. In order to help understand the current state of policy development we will define key dimensions for each policy aspect. Figure 1 (Appendix B) illustrates a proposed set of five policy aspects and their associated dimensions. This section addresses the current state of each dimension and offers a specific example with a short description of the potential interactions with other policy levers.

Cyberspace civil rights refers to the rights U.S. citizens should expect to maintain in the cyber environment. The primary dimensions are privacy, net neutrality and access. Privacy is a significant legislative issue. The amount of personal data collected and stored in networks is significant and growing exponentially. Governments wrestle with the level of privacy individuals should have a right to expect on the internet. The U.S. and EU legislative forums have addressed this issue and offered differing policies that could further exacerbate the complexity of the issue. Additionally, proposed legislation on net neutrality addresses concerns of consumers and content providers. Some industry representatives believe the legislation needs to be modified to expand network providers' ability to actively manage data traffic. Current legislation appears to limit the ability of network providers to manage traffic in order to allow acceptable quality of service. Finally, the broadband access plan attempts to ensure low user density areas like rural America retain affordable, high speed access to internet services.

Security policy is somewhat disjointed. While the federal government has enacted the Federal Information Security Management Act (FISMA) and has taken steps to secure government networks, private sector standards are spotty and enforcement is ineffective. "The network's interconnected nature makes them vulnerable to failures and widespread consequences. Secure and reliable operations of these systems is fundamental to our economy, security and quality of life."[12] This interconnectedness with ICT adds tremendous complexity to the government policy question. "Attacks on Critical Infrastructure and Key Resources (CIKR) could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident."[13]

Competition addresses the ability of firms to compete within the U.S. and globally. Both international trade issues and U.S. policies affect competition. The U.S. is currently attempting to manage Radio Frequency (RF) spectrum for the wireless telecom industry. These attempts have resulted in a competitive landscape resembling the most gerrymandered of Congressional districts. Government continues to draw lines and make policy distinctions that technology has long since made irrelevant. This is evident in artificial distinctions between wireline telephone, cable television, and wireless service providers. Government policy still treats many aspects of these industry segments as unrelated and separate when they are in fact converging.

Connectivity refers to the ability to provide high capacity access to resources available in the network using wireline and wireless products. Currently, the U.S. manages RF spectrum in a largely command and control fashion. This is due to the fact that, "The basics of the system we use today were established when the most important use of spectrum was broadcasting and the range of usable spectrum was about 1% of what it is today."[14] Additionally, wireline communications continue to play a significant role as the ICT backbone. Whether copper twisted pair loops, fiber optic, or coaxial cable, wired communications enable many industries including telecommunications, Voice over Internet Protocols (VoIP), cable television, Internet Service Providers (ISP), satellite television, wireless backhaul support, and undersea high-speed/high-capacity intercontinental data connections via submarine cables.[15]

Innovation refers to the ability of the ICT industry to develop new technologies and associated products. The primary dimensions are research and development, IPR and human resource management. Currently, a 50/50 split exists between government and private funding of R&D. "The role of the federal government facilitating innovation in the ICT sector has been absolutely critical in supporting a robust ICT research ecosystem, both through direct federal investment in ICT research and facilitating commercialization and private research investment."[16] Globally, IPR affects the U.S. ability to compete and conduct R&D. In May 2011, the U.S. Trade Representative released the finalized text of the Anti-Counterfeiting Trade Agreement (ACTA). This multilateral agreement, negotiated outside the World Trade Organization (WTO) with nearly 40 advanced industrialized nations, expands upon the WTO Trade-Related Aspects of IPR (TRIPS) protections to specifically address the challenges of digital counterfeiting and piracy. Since the public release, Australia, Canada, the European Union, Japan, South Korea, Morocco, New Zealand, Singapore and the U.S. have all signed ACTA.[17] Finally, in response to an increasingly litigious and protracted patent administration environment, Congress enacted the Leahy-Smith America Invents Act (AIA) on September 16th, only the fourth major revision of patent law since 1793. Aimed at addressing the patent "explosion,"[18] AIA changed the U.S. from the only major nation employing the "first-to-invent" date for judging an invention's novelty and obviousness to the "first-to-file" standard used by the vast majority of nations.[19] Additionally, the AIA "created several new patent-review processes with a goal of reducing the number of questionable patents" and made it more difficult for non-practicing entities to exploit the patent system.[20]

Despite these many policy challenges the ICT industry is still very healthy. However, maintaining this health requires senior leaders to examine the numerous incongruities created as industry innovation dramatically outpaces government policy and government's basic understanding of the industry.

Chapter IV: Challenges

The ICT industry is a principal engine of innovation-based economic growth feeding the U.S. and international economies. Much of the U.S.'s comparative advantage in the information age is linked to the effective employment of cyberspace and a healthy ICT industry. Averting a potential "tragedy of the commons" in cyberspace is of critical interest to the U.S. government, which faces significant policy challenges that threaten the positive externalities generated by (1) cyberspace freedom, (2) cyberspace security, (3) connectivity, and (4) U.S. competitiveness. The inherent interconnectivity of cyberspace creates a complex web of interrelationships.

Challenges in Cyberspace Freedom: The rate of change in innovation within cyberspace and the ICT industry far exceeds the pace of the U.S. legislative and regulatory processes. Many current telecommunications laws and policies are outdated and no longer produce the intended result. Some ICT firms use these antiquated regulations as a core component of their business model, eroding competition, innovation, and creation of public value.

Privacy: Control and ownership of data is a topic of ever increasing importance. Centralized cloud computing offers gains in efficiency and productivity but at a cost in centralized control. This centralization also provides tremendous environmental benefits as data centers consolidate into energy efficient facilities. The ICT industry challenge is to develop norms and standards which protect privacy of individuals, firms, and governments while still enabling efficiencies.

Net Neutrality: A natural tension exists between the legitimate need of ISPs to manage their networks in order to maintain contracted service levels across their paying subscriber base and individual users who expect unfettered, content-neutral internet access on demand. On 21 December 2010, the FCC released a Report and Order, FCC 10-201, titled "Preserving the Open Internet and Broadband Industry Practices." This report lists internet transparency, no blocking, and no unreasonable discrimination as pillars for maintaining network neutrality. Implementing network management policy in an environment characterized by rapidly increasingly demand for large data flows with low latency will further amplify the inherent tension with net neutrality.

Cyberspace Access as a Human Right: With more than two billion users, cyberspace has become an indispensable domain that undergirds the global economy and connects distant corners of the world. In an era where information is the foundation for the creation of economic value, unfettered access to this domain is a fundamental issue of human freedom of expression on par with the basic human rights of freedom of speech, assembly, religion, and the press. International recognition of this right and the preservation of free access in opposition to governments, who would use the internet as a tool for repression, is a significant challenge.

Challenges in Cybersecurity and Critical Infrastructure Protection: Maintaining the integrity, availability, and confidentiality of information in cyberspace against denial, theft, alteration, or attack is arguably the greatest challenge facing this domain. In his 2010 National Security Strategy, President Obama states, "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation."[21] A detailed analysis of cybersecurity is provided on page 18.

Challenges in Connectivity:

Wireless Spectrum Availability: Absent a breakthrough in modulation technology, the limited radio frequency spectrum licensed by the FCC to the commercial wireless industry is insufficient to meet future requirements and represents a significant barrier for entry into the wireless service industry. Industry is actively engaged in deploying fourth generation digital cellular networks using the Long Term Evolution (LTE) International Telecommunication Union (ITU) standard and attempting to more efficiently employ currently licensed spectrum with smaller and smaller cells and other frequency re-use schemes. Additionally, wired providers are attempting to develop session switching technologies to allow the employment of unlicensed WIFI spectrum to meet demand. The U.S. government needs to develop a modern scheme to more efficiently and effectively monetize spectrum in order to mitigate the scarcity issue.

Challenges in Competitiveness:

Research & Development (R&D): The U.S. ICT industry's remarkable, innovation-based growth has benefited from robust R&D investment. While government spending on R&D over the last three decades increased in constant year dollars, it has not kept pace with GDP growth. The U.S. has fallen from first to seventh place among Organization for Economic Cooperation and Development (OECD) countries in R&D intensity and the ratio of R&D expenditures to GDP. This threatens the competitiveness of the U.S. ICT industry and the economy as a whole.[22]

Human Capital: The more than four million people working in the U.S. ICT industry are an important source of innovation and entrepreneurial spirit, enabling advances and efficiencies in other industries. However, attracting the best and brightest into the ICT industry is becoming increasingly challenging as companies compete against other sectors (such as financial services and consulting) for top talent. Despite the high national unemployment levels, ICT companies are increasingly experiencing long term position vacancies because of a mismatch in skills. Skilled foreign-born workers with H-1B visas fill some positions, but this program has annual limits and it was never intended to be a path to citizenship. Government faces even greater challenges in hiring top talent, often needing to find people both willing to work in its more restrictive environment and capable of meeting security clearance requirements.

Social Networking: Social networking has had an overwhelming impact on business practices. In addition, during the 2008 presidential election, the Obama campaign successfully used social networking to gain popular support and raise record setting amounts of campaign funds. We are already seeing the next logical progression to national security impacts. However, government lags in overall adaptation of Web 2.0.[23] The hierarchical practices of traditional government have not kept pace with the upsurge in social networking systems.[24] The proliferation of social software has ramifications (beyond productivity and capability) for U.S. national security and has been leveraged to achieve significant results.[25]

Chapter V: Industry Outlook

Going forward, the ICT industry does face significant challenges. The industry outlook is shaped by a continued convergence of capabilities driven by a growing demand for increased data both in terms of storage and distribution. These demands are driven by market realities, policies and legislation.

Several of the vulnerabilities of the industry lay in its global supply chain, as evidenced by flooding in Thailand and the subsequent impact on the hard drive market. Counterfeit or modified hardware discoveries have exposed additional vulnerabilities in global hardware supply chains. The U.S. ICT industry could also be vulnerable if companies move a greater percentage of their business overseas due to more favorable tax rates and to be nearer to manufacturing centers, innovation centers, and less expensive labor. This can be seen in Vietnam where labor costs and favorable tax policy have begun to attract top U.S. firms such as Intel and IBM along with top Chinese firms such as Huawei. This strategy to capitalize on emerging nations such as Vietnam is commonly referred to as a "China +1" strategy. Vulnerabilities to this are best addressed through government and industry partnerships/dialogue on common standards.

Social networking continues to play a large role throughout society with movements such as the Arab Spring and Occupy Wall Street leveraging social media in ways not previously seen. Government policy makers need to develop a comprehensive and balanced plan to embrace social networking as a strategic communications and productivity tool. Even after the Arab Spring, anecdotal evidence in Vietnam, Hong Kong and mainland China suggests the power of social networking has only just begun to materialize.

The current trend in data and communication clearly leans toward a preference for mobility. While it's impossible to predict innovations in specific devices (or the development of new devices), we can say competition for spectrum will skyrocket. Absent policy reform, antiquated spectrum allocation policies and increased consumer demand will continue to squeeze this limited resource. Current FCC/National Telecommunications and Information Administration (NTIA) policy produces short term solutions which struggle to keep up with consumer demand and national security requirements. The exponential move to mobility and wireless necessitates a change from 20th century industrial age command and control policy to 21st century information age flexible policy. In the medium to long term this means we should seriously look at reducing government's role in regulating spectrum to allow for more efficient, market driven allocation of resources.

While wireline connections have flattened, they continue to perform well in markets such as rural areas with limited wireless support, densely populated urbanized areas where wired deployments are in place and return on investment is higher, as well as business where there is demand for speed, bandwidth, connection consistency and quality.[26] Additionally, wired support to wireless networks via backhaul is expected to rise 8-15% per year through 2015. Finally, the wired undersea cable industry has seen its business grow in quantity, capacity, and importance as globalization has increased dependence on intercontinental communications.

In the short term (0-18 months), the ICT industry will experience a shifting focus to mobile computing with an explosion of smart phones and tablets driving demand for more wireless data capacity. Recent EU privacy policy and focus on intellectual property through the proposed Stop Online Piracy Act/PROTECT Intellectual Property Act legislation will continue to influence the industry. The current government focus on cybersecurity and political necessity to create legislation will have an impact on the industry. However, policy makers must also recognize that excessive legislation could produce the opposite of the desired effect.

The medium term (18-36 months) will continue trends toward the "post PC world" and "bring your own device" with businesses embracing new methods for employees to connect to networks and boost productivity. Moore's law predicts continued rapid increases in technology driving shortened development cycles and exponential growth in bandwidth requirements. As the "core device" markets for PCs and servers become increasingly commoditized, connectivity continues to stretch out into other sectors.

The long-term (3-5 years) will continue the trend toward an "Internet of Things" with increased machine-to-machine connections. These interactions will become more commonplace as "smart grid" technology and the connectedness of products and services to the internet continues to become more ubiquitous. Looking beyond 3-5 years in the ICT industry is futile. The smart phone is just one example of a technology which was developed and completely transformed global commerce and communication well within a five year timeframe.

The U.S. comparative advantage in the industry is driven by innovation. China has the capacity and inexpensive labor to produce goods and even copy U.S. goods, but until recently lacked the capability to innovate on a significant scale. Chinese companies such as Huawei are now producing new products of similar quality to their traditional U.S. competitors. The U.S. will continue to dominate higher end ICT innovation, but with increased competition. However, lower end jobs ("ditch diggers" of the ICT industry) will continue to migrate to developing markets in Vietnam and throughout Asia. This trend cannot be stopped in the U.S. or in China. Value is created in the U.S. ICT industry by continually pushing the envelope at the top end.

In addition to Asia, Africa is another significant market gaining great focus. If the U.S. is not careful, Chinese firms could easily end up controlling the IT infrastructure, consumer devices, and access to information (both content and the ability to affect public opinion/government policy) throughout the African continent. African consumers already use wireless phones for financial transactions. Advances in health care made possible by mobile units are connecting poor areas of Africa with top-notch medical doctors. Some U.S. companies are positioning to grow in the African market by targeting low cost devices. We see a similar trend to that of Asia where developing countries skipped the traditional personal computer in favor of mobile computing capability. The market in Africa will be defined by low cost mobile computing. Of significant concern though is the Africa strategy of top Chinese ICT firms. Both Baidu and Huawei appear to be fully focused on expanding into Africa and other underdeveloped regions. The national security implications of such a move warrant serious consideration.

Many nations are rapidly retooling their economies to produce technologically advanced products and services through investments in R&D.[27] Nations around the world have introduced tax benefits, subsidies, science-based industrial parks, and worker-training programs to lure the owners of high-technology manufacturing and R&D facilities. China uses these tools and its enormous market to encourage technology transfer to Chinese partner companies.[28] Competition from Chinese telecom companies ZTE and Huawei is increasing as China focuses more on internal R&D. "Huawei allocates almost half of its 140,000 staff to research and development."[29] By comparison, Oracle, with 108,000 total employees worldwide, dedicates 30,000 to R&D.[30] Furthermore, although the U.S. has been one of the world's hottest smartphone markets during the past few years, it will likely be surpassed by China by the end of the year. "Due to their sheer size, strong demand, and healthy replacement rates, emerging markets are quickly becoming the engines of the worldwide smartphone market."[31] Where the engines are, so will go the fuel (i.e. the money) as R&D investment shifts to the markets with the greatest profit potential.

Chapter VI: Government's Role

The role of government is a contested and often misunderstood issue. ICT firms contribute more than $1 trillion to U.S. GDP, account for more than four million jobs, and are significant contributors to U.S. productivity gains.[32] As a vital component to the U.S. economic engine, government involvement within the industry must be approached cautiously, striking a balance between stimulating and protecting the industry without burdening or stifling its development. Figure 2 (Appendix B), highlights how government should look at its role compared with current policy. Aspects of these policy levers are discussed in more detail below.

In a paper on communications infrastructure, the OECD detailed three roles government can take: (1) a stimulator focused on removing barriers, (2) a producer through direct investment and (3) a regulator, fostering a competitive marketplace and protecting consumer rights.[33] These roles provide a framework for discussing the role of government within ICT. The following discussion of these areas encompasses information extracted from individual research into specific ICT issues as well as data gleaned during trade association and firm visits.

Stimulate: The most prominent characteristic of ICT is its dynamic nature, constantly reinventing itself with new technological breakthroughs and innovations. Stimulating that development is an area where measured and thoughtful government involvement can be beneficial.

1) Foster R&D: Considering the U.S. dependence on ICT products, the government must ensure adequate R&D investment in both basic and applied research, particularly in areas whose functions are unique to government. Government action can take the form of tax benefits such as a permanent R&D tax credit, decreasing the corporate tax rate, and allowing repatriations of money sheltered overseas with R&D investment requirements. It can also be accomplished through grants and subsidies such as the Wireless Innovation Fund. Finally, it can be encouraged through support of public/private consortia & regional clusters designed to seek equal participant investment toward a common technical goal.
2) Incorporate Social Networking Within U.S. Government: Social networking provides an internal and external collaboration tool for the U.S. government. However, despite its popularity and potential, most agencies have been slow at effectively integrating its use. The lack of adoption of social networking tools betray a significant cultural resistance within the U.S. Government to transparency, open communication, and data-centric decision making within the bureaucracy. Significant cultural obstacles to adoption of Information Age tools and techniques represent a critical leadership challenge, but also the potential for dramatic improvement in government services and public trust.
3) Develop ICT Human Capital: Lack of sufficiently educated/trained ICT personnel is one of the factors driving U.S. ICT jobs overseas. To improve access to U.S. educated ICT workers, the government should; (1) facilitate effective education programs, K through college in all areas (not only STEM); (2) increase the use of summer internships and fellowships within government (specifically the lab system); (3) create a government website for H-1B employers to post notices of their intent to initiate H-1B petitions; (4) modify the H-1B program to return it to its original purpose of filling short-term employment needs rather than as a path to immigration; and (5) offer a separate program to provide a path to citizenship for highly motivated foreign-born students interested in remaining in the U.S.

Invest: While not always the most efficient or effective approach, there are circumstances where direct federal investment is warranted. This is particularly appropriate when dealing with unique capability requirements (often times classified) within the DoD and Intelligence Community (IC).

1) Direct R&D Funding: The federal government directly funds ICT research through a number of departments/agencies such as the National Science Foundation and other DoD laboratories. Additionally it funds supercomputer development utilized by agencies such as DoD, Department of Energy, NASA and the IC. Continued support of U.S. ICT research is vital to maintaining U.S. cutting-edge ICT capabilities in support of U.S. national security objectives.
2) Support International ICT Development: U.S. DOS has dedicated $50 million in foreign assistance funds since 2008 to protect internet freedoms in more than 40 countries around the world where governments are taking steps to restrict internet access.[34] Given the significant role internet access and social media played during the Arab Spring, such programs must

continue. Doing so capitalizes on the strengths of the ICT industry in support of the U.S. National Security Strategy.

3) Broadband Deployment: Continue support for the National Broadband Plan to ensure the benefits of high-speed Internet access are enjoyed by all, including those living in rural areas.

Regulate: The challenge for ICT policymakers is to develop policies which address issues but contain flexibility to accommodate future changes in technology.[35] This is even more vital as 20th century industrial age governments attempt to keep pace with a 21st century information age economy. The most effective means of accomplishing this is to partner with industry on common solutions rather than directing government-developed solutions.

1) Cyber Security Strategy: Currently, there is no comprehensive cybersecurity strategy with a common set of internationally-accepted standards defining the level of security private sector organizations should use for their computer systems. Standards should take into account tailored network requirements based upon the sensitivity of information, guidelines for assessing cyber preparedness and a notification system to inform customers of infections and intrusions along with tools to fix problems. The time for such a strategy has come and the solution lies in a partnership approach bringing in expertise from industry, academia, and government. Domestic cybersecurity initiatives must be a part of a longer trajectory that focuses on multilateral standards and agreements, rather than arbitrary, unilateral domestic regulation. Any cybersecurity policy worthy of consideration within U.S. Government agencies, and any cybersecurity law worthy of consideration by the U.S. Congress is worthy of energetic multilateral dialogue.
2) CIKR Recovery: Critical infrastructure resiliency and recovery requires extensive prior planning. To facilitate these plans, government leaders should enact policy that uses industry mechanisms to implement and govern firm behavior. First, governance policy should provide transparency for consumers of ICT services to understand standards implemented and the level of risk mitigated by the backend ICT services. Second, government must manage risk and provide an agile mechanism to govern the risk assessment. Finally, ICT providers must be held liable for an accepted level of service to each CIKR category.
3) Wireless Spectrum: The wireless spectrum is in high demand. To maximize the efficiency of its use, industry experts and government officials should closely examine the proposal put forth by Faulhaber and Farber regarding wireless spectrum allocation. The solution balances innovation and free market economics with the need to offer certain valuable public goods via wireless services.[36] Subsequent spectrum policy should be developed (1) with the agreement that emergency and government-type services must have priority during a crisis, (2) to reflect the reality that technology will change faster than policymaker's ability to rewrite policy, and (3) in coordination with international agencies to avoid conflicts.
4) Cloud Computing: The GSA set up the Federal Risk and Authorization Management Program (FedRAMP) to "create a uniform set of security requirements for cloud providers."[37] The goal is to provide a single certification to cloud service providers to reduce costs of agencies looking to move services to the cloud. This should be evaluated as a government-wide standard, in coordination with any available and applicable industry standards.
5) Continue IP Policy Growth: To further enhance U.S. IP policies, a number of actions should be taken. First, Congress should pursue counter-piracy legislation along the lines of OpenDNS that has ICT industry support and does not undermine Domain Name System (DNS) security. Second, the President's export control system reform proposal needs to be accelerated past

phase I and expanded to address the GAO's high risk recommendations. Third, the Intellectual Property Enforcement Coordinator should revise the joint strategic IP enforcement plan to incorporate both DoD participation and the President's vision for export control reform so that these equities are properly represented. Fourth, the administration should leverage the momentum built by ACTA to work within the WTO framework to update TRIPS to better address IP protection in the digital environment. Finally, the Congress should create federal trade secret protection legislation to both attain uniform protection for this important IP class and coherent management across the IP policy classes.

6) Decrease Manufacturing Supply Chain Risks: The U.S. government's current programs, like Customs-Trade Partnership Against Terrorism**,** do not address national security equities within computer and network equipment manufacturing. The industry's partnering solutions, like the Trusted Technology Forum, and ISO standards of practice represent more complete, effective, and sustainable solutions to supply chain security threats. The U.S. government must partner with industry and use its unique special technical capabilities to monitor supply chains in an oversight mode. Furthermore, the government should expand the Trusted Foundry Program high-volume, cost-driven infrastructure at the enterprise level for its own acquisitions.

Chapter VII: What can Government Learn from the ICT Industry?

Government can and should learn from several ICT commercial best practices. This chapter identifies themes and practices observed consistently in top performing ICT firms. In addition, top workers identified these best practices as expected conditions of employment. Government leaders must champion the cultural changes required by the information age.

A Culture of Collaboration: By far, the most significant observation of the high-performing industry leaders is the infusion of a pervasive culture of collaboration. This culture manifests itself in various forms. First, firms adopted network and cloud based collaboration and social media suites. In larger firms, the systems were internally developed and allowed users to share project-specific information, identify and manage talent, host discussion forums and share general company information. A second manifestation of the culture of collaboration was the routine, easy use of video. The video conferencing hardware and software was integrated into their collaboration software and even their business productivity software. Additionally, the personnel overhead necessary to support video conferences was minimal.

An Untethered Workforce: A consistent observation is that top performing companies have fully embraced the information age model of working remotely (aka "telecommuting"). Even at the largest multinational companies, it was common to see telecommute rates as high as 40%. Three conditions appear to enable successful telecommute models. First is the culture of collaboration discussed above. Second is a culture of trust that employees will produce. Finally, these firms use metrics to measure performance output instead of considering the 40-hour work week as an output. Several executives stated they observed increases in both hours worked and productivity for employees who telecommute.

Control Security Instead of Letting it Control You: The top firms learned over time to manage ICT security vulnerabilities and risks instead of letting security requirements restrict how the organization operates and conducts business. Through robust and effective risk management practices, top firms are better able to make value judgments and tailor appropriate levels of security to identified and measurable risks.

Efficient Use of Resources: Conservation of energy surfaced as a top priority. Interestingly, the largest data centers in the world are run well above 80 degrees Fahrenheit. At these high temperatures leading firms expect a small, but measurable number of hardware failures.

However, powerful data analytics has shown the cost of just a few hardware failures (and built in redundant processing) is dwarfed by the energy savings. Energy efficiency was a common theme in the U.S. and during field visits in Vietnam, Hong Kong, and mainland China.

In summary, while the government plays a key role in setting policies conducive to benefiting industry, there are ample opportunities for the government to take lessons from industry best practices in collaboration, productivity, security and energy efficiency.

Chapter VIII: Essays

Governance: As stated in current conditions, a national strategy and a set of governing bodies is needed to organize IT efforts across the nation for the betterment of the U.S. economy and national security. The National Broadband Plan, electromagnetic spectrum management, and network neutrality efforts, along with Federal and Department of Defense IT governance contain some positive steps toward creating structure.

National Broadband Plan (NBP): As part of the American Recovery and Reinvestment Act of 2009 Congress tasked the FCC to develop a NBP to "ensure that all people of the United States have access to broadband capability."[38] The FCC completed the plan on time and delivered it to Congress in March 2010.[39] The NBP outlines a strategy for treating broadband service as an essential utility for all Americans, as essential as electricity, and to increase its throughput performance and push it out across the nation at an affordable price.

The NBP makes four recommendations to the Executive Branch, Congress and state and local governments. The FCC also proposed six long-term goals for achieving Congress's vision, with the most prominent and challenging goal of providing affordable internet access to over 100 million U.S. homes at download and upload speeds of at least 100 and 50 megabits per second.[40]

To expand broadband use in rural areas of the country, the U.S. Department of Agriculture also plays a governance role through the Rural Utilities Service and its Broadband Initiatives Program to provide grants, loans, and loan guarantees with the $7.2 billion allocated by Congress in 2009.[41] In the Recovery Act of 2009, Congress also appropriated $4.7 billion to NTIA for implementation of the Broadband Technology Opportunities Program (BTOP), which is designed to help states, non-profit organizations, and broadband providers further deploy broadband capability.[42] The BTOP places special emphasis on extending access to healthcare, education, and children through disadvantaged small businesses.[43]

Spectrum Management: One of the most important elements of the NBP is in the area of spectrum management. Critics have described the FCC's management of spectrum in the past as being ad hoc, allocating on a band-by-band, service-by-service basis.[44] With the sudden increase in wireless broadband use, the FCC realized wireless broadband expansion would be limited unless they could identify additional spectrum and develop a better management approach. The FCC determined they needed to make available 500 MHz of spectrum over the next 10 years, with over half needed within the next 5 years for mobile use.[45]

In the NBP, the FCC recommended, and Congress granted, the NTIA authority to impose fees on spectrum license holders and government spectrum users.[46] The Middle Class Tax Relief and Job Creation Act of 2012 contains Title VI – Public Safety Communications and Electromagnetic Spectrum Auctions.[47] The primary components of Title VI provide for the reallocation of public safety spectrum, governance over it, authority for FCC auctions, and a mandate to review federal spectrum for reallocation.[48]

In the public safety sections of the Act, Congress directs the reallocation of the 700 MHz D-block spectrum to public safety in return for the current public safety bands, i.e. 470-512 MHz, for competitive auction.[49] It also establishes a governance structure that consists of a

Technical Advisory Board for First Responder Interoperability under the FCC; a First Responder Network Authority (FirstNet) within the NTIA; and a standing FirstNet Public Safety Advisory Committee consisting of agency, consultants, and industry experts.[50]

The Act defines FirstNet responsibility as to "… take all actions necessary to ensure the building, deployment, and operation of the nationwide public safety broadband network, in consultation with Federal, State, tribal, and local public safety entities, the Director of NIST, the Commission, and the public safety advisory committee…[51] FirstNet has authority to carry out these responsibilities, but must work through a board that consists of the Secretary of Homeland Security, the U.S. Attorney General, the Director of the Office of Management and Budget and 12 members appointed by the Secretary of Commerce.[52]

The Act also calls for the NTIA to work with the Department of Defense (DoD) and other parts of government to identify spectrum that can be moved to or shared with the commercial sector.[53] There are also broader inferences to reallocating spectrum that may impact government. For example, section 6410 of the Act assigns responsibility for promoting "… the best possible and most efficient use of electromagnetic spectrum resources across the Federal Government subject to and consistent with the needs of the missions of Federal agencies."[54] However, the DoD is not a voting member on any of the spectrum management governing bodies, which may open it up to decisions made without having direct input into the process. Spectrum management is an area where the DoD stands to lose the most.

Network Neutrality: On December 21, 2010, the FCC released a Report and Order, FCC 10-201, Preserving the Open Internet and Broadband Industry practices, to take what it said was, "… an important step to preserve the Internet as an open platform for innovation, investment, job creation, economic growth, competition, and free expression."[55] The report contained a section titled "Preserving the Free and Open Internet" that listed internet transparency, no blocking, and no unreasonable discrimination as pillars for maintaining network neutrality.[56]

The FCC published these rules and tied them to the NBP for what they describe as a means of empowering and protecting consumers and innovators "… while helping ensure that the Internet continues to flourish …"[57] The report states that the comments received from industry experts, academia, and consumer advocacy groups were used to formulate the rules.[58] Through their public requests for comments they noted that "Commentators agree that the open Internet is an important platform for innovation, investment, competition, and free expression, but disagree about whether there is a need for the Commission to take action to preserve its openness."[59] Primary internet service providers largely believed new regulations were not needed, were too costly to implement, and market and consumer pressures would keep providers from unreasonably restricting internet openness. The FCC ultimately believed rules, and enforcement of them, were the better approach.[60]

Prior to the Open Internet order, the FCC ruled that Comcast had violated its 2005 internet non-interference policy when Comcast blocked peer-to-peer connections to better manage the network traffic.[61] Comcast disagreed and, in August 2008, filed an appeal with the U.S. Court of Appeals for the District of Columbia, claiming the FCC did not have the statutory authority to make or enforce such rulings.[62] The Appeals Court agreed with Comcast and vacated the order in April 2010.[63] Within the year of the Court decision, the FCC published their latest set of rules in Report and Order, FCC 10-201.[64]

Since the release of the FCC's latest Net Neutrality order, Verizon, MetroPCS Communications, and CTIA-The Wireless Association have all filed suit challenging the FCC's authority to regulate the internet.[65] On the other side of the argument, several consumer advocacy groups have filed suit saying the FCC was not going far enough because they limited their ruling to wireline carries and did not apply the same standards for wireless internet access.[66]

Although Comcast won its appeal, they continued to adhere to the original ruling. Additionally, Verizon and Google proposed a set of net neutrality guidelines that all providers could live with, but they were quickly rejected by the FCC.[67] Providers believe government regulations over the internet will do more harm than good and that market and consumer driven pressures will keep providers in check.[68] History in the regulation of the electricity industry, wired telephone services, the transportation industry, and many others that were heavily regulated lends credibility to their argument.
- Mr. Daniel Fri, Dept of the Air Force

Spectrum: Spectrum management within the wireless industry is a microcosm of overall inept government attempts to regulate 21st century industry with 20th century policy. The FCC authored the NBP in an attempt to map out a way ahead for key issues, including aspects of the wireless industry. "Thirty-six public workshops held at the FCC and streamed online, which drew more than 10,000 in-person or online attendees, provided the framework for the ideas contained within the plan. These ideas were then refined based on replies to 31 public notices, which generated some 23,000 comments."[69] This does not however mean the solutions and policies adopted/contemplated by the government are sound. Instead, the current state of regulatory affairs surrounding the wireless industry reflects a consensus that is both politically palatable to government and profitable for the key industry leaders and groups.

To better understand the health of this industry (and spectrum management) and the effects of government regulation we turn to Porter's "Five Forces."[70] Analysis of threats from new entrants, substitute products, and competitors as well as the power of buyers and suppliers reveals this to be a healthy industry. However, looming changes in the competitive landscape and regulatory environment do hold the potential to cause major upheaval. Absent technological advancements, consumer demand for spectrum is outpacing the available supply. "Wireless subscribership has increased dramatically over the past decade, from 97 million in June 2000 to almost 293 million in June 2010."[71] Furthermore, the iPhone is causing significant economic pain to the industry leaders. Verizon averaged EBITDA service margins of 46.4% per quarter in 2009 and 2010. After offering the iPhone those margins dropped to 43.7% in the most recent quarter. AT&T is suffering a similar fate falling to 28.7% compared with 37.6% a year earlier. If left unchecked, this trend could erode the attractiveness of the wireless industry and lead to a rewriting of the industry business model.

High barriers to entry help maintain the dominant positions of industry leaders. Consumer preferences for mobility discourage substitutes and help to keep prices from dropping to commodity levels. While both buyers and suppliers have gained significant power, the industry is still very profitable. "Revenue in 2011 is projected to total $195.8 billion, a 4.4% increase from 2010. Over the past five years, revenue has grown an average of 5.0% per year. Profitability has grown as well; operating margins among the major players increased from 14.7% in 2006 to 20.8% in 2011."[72] However, one key factor looms large as a significant threat.

Limited availability and, in many cases, inefficient allocation/use of RF spectrum must be addressed. Proper government policy and oversight is required to ensure RF spectrum and wireless services/capabilities are available to meet both consumer demand and government availability in times of crisis. Policy should take into account the increased demand for consumer mobility, expanded machine-to-machine communication (auto industry, utility monitoring), new healthcare applications, enhanced public safety requirements (E-911 and emergency responder requirements), and national security concerns. Furthermore, the global nature of commerce and worldwide presence of America's Armed Forces means we cannot make policy decisions in isolation.

The major challenges to the wireless industry and users of spectrum in general, are a perceived scarcity of resources which has been exacerbated by government's inefficient management of the resource. This is partly due to the fact that, "The basics of the system we use today were established when the most important use of spectrum was broadcasting and the range of usable spectrum was about 1% of what it is today."[73] The government doubled down on these antiquated policies with the recent passing of the Middle Class Tax Relief and Job Creation Act of 2012. Within this legislation, the U.S. attempts to essentially create a mirror image of the current commercial wireless network and use it to provide emergency services. A former chief economist at the FCC appears to agree with this claim in his writings.[74] The current policies and proposed solutions, including voluntary incentive auctions, are a continuation of these same practices. They fail to address long term reforms and the current state of technology.

First, on the issue of scarcity, "A limited 2005 study for the National Science Foundation surveyed the spectrum from 30MHz to 3GHz at six locations (five urban and one rural), finding all the spectrum almost completely unused. In the rural test, occupancy was only 1%, and in the most used location (in New York City), occupancy was only 13%."[75] These statistics shed light on what may become available with a combination of sound market-based management practices and further technological developments. Policy must reflect the reality that future technology is likely to make the current paradigm for allocating spectrum obsolete.

20th century arguments in favor of tight control by the FCC are not economically sound. Ronald Coase (awarded the Nobel Prize for his analysis of spectrum allocation), "suggested that it would be better if use of the spectrum was determined by the pricing system and was awarded to the highest bidder."[76] In attempting a free market solution, the FCC and some industry leaders tout the idea of voluntary incentive auctions. However, these auctions are unlikely to attract new major players or spur innovation.[77] In addition, economic analysis suggests the maximum valuation for spectrum is realized absent conditions or restrictions on bidders.[78] One alternative could also be large scale open access. This however invites the tragedy of the commons where the resource is overused. The result is that spectrum becomes largely useless to all. [79]

The critical question in all this discussion still concerns the best mechanism and incentives to ensure efficient allocation of wireless services. At the same time, we wish to preserve some amount of emergency/crisis and national security capability regardless of how market forces change. Gerald R. Faulhaber, University of Pennsylvania's Wharton School and David J. Farber, Carnegie Mellon University have outlined just such a solution worthy of additional consideration. This solution balances innovation and free market economics with the need to also offer certain valuable public goods via wireless services. It also recognizes that the process by which we got to this point is broken and has resulted in an inefficient allocation of resources. The basic outline of this solution is show in Appendix C. [80]

The wireless industry is profitable and is creating value. The main challenge faced by all users of spectrum was created through ineffective government oversight. Government is attempting to remedy the situation via additional 20th century style regulations. As two noted experts on the subject state, "Perhaps the closest analogy to the U.S.'s current approach is that of GOSPLAN, the central planning agency in the former Soviet Union."[81] We are in effect tinkering around the edges with (grossly underfunded and technically impractical) set asides for

things like emergency services. In other instances we are wedded to frequency allocations for specific military or commercial uses simply because they got there first. The current national plan does not solve the long term problem or address the root causes. Anarchy and complete unregulated open access is not the solution. The solution is a free market with light regulations which removes heavy handed FCC/NTIA control. An engineering study of actual spectrum use and a Nobel Prize winning economist have pointed in the same direction. Government has created the problem. We can solve it by building a smartly regulated 21st century free market.
- Lt Col Thomas Falzarano, U.S. Air Force

Human Capital: The driving force behind the growth in the U.S. ICT sector is its highly skilled and innovative workforce. Sustaining such growth, however, depends on the continued availability of such individuals. Based solely on the number of U.S. graduates in STEM fields (three times the number of job openings) [82] accomplishing this task would appear within reach. Yet U.S. ICT companies consistently claim difficulties hiring people with the right skills and experience, leading to assertions of shortages in the STEM workforce and calls for loosening restrictions on immigration of highly skilled workers to fill the gap. The competition to hire the "best and brightest" occurs not only within the ICT industry but also with other industries, specifically finance and consulting.

H-1B visas are for nonimmigrant, temporary workers in response to short-term employment issues. One misconception about the program is that companies must first try to find qualified Americans before turning to an H-1B. In fact, according to the U.S. Department of Labor, there is no such requirement.[83] Since FY2004, the annual limit for initial H-1B visa petitions has been 65,000. This number does not include renewals or changes and exempts universities and affiliated nonprofits, nonprofit research organizations, and governmental research organizations. In addition, a 2004 reform allows 20,000 H-1Bs for graduates of U.S. universities with a master's or higher degree. As a result, the actual number of H-1B visa petitions granted in a year is substantially greater than the nominal 65,000 limit.

In FY 2010, the latest year for which numbers are available, 192,990 petitions were approved for both initial employment and continuing employment out of 247,617 filed.[84] The numbers show year-over-year decreases since at least FY 2007. Possible reasons for at least a portion of the decline are the recession and the extension of some F-1 student visas.[85] Of the petitions, by far the most (53.3%) were from India. India-based Infosysy Technologies, for example, a company consistently at or near the top of the list of companies using temporary worker visas, received 3,800 H-1Bs and some 2,300 L-1s in FY 2010.[86] The next closest country in terms of petitions was China with 8.9%.[87]

Known characteristics of the applicants granted H-1B status include age (68% are between 25 and 34 with 54% of initial applicants under 30), education level (42% bachelor's degree; 39% master's degree), occupation (47.5% in computer-related occupations), and compensation level (median for computer-related occupations was $71,000 compared to the median overall level of $68,000).[88] ICT sectors making use of H-1Bs include computer systems design and related services, computer and peripheral equipment manufacturing, and communications equipment manufacturing were. The most visa approvals were for computer systems design and related services (36%).

There are two schools of thought about the role of H-1B visas in the ICT industry. Proponents recommend either increasing the annual cap or replacing it with a market-based cap to allow foreign-born skilled workers to fill gaps in the U.S. workforce. They state H-1B visa holders do not take jobs from American workers and in fact, create jobs. Critics assert such visas are not necessary, citing U.S. unemployment levels and statistics showing no relationship between H-1B visas and job creation. For example, between 1999 and 2007, enough H-1B computer worker visas were approved to fill 87% of the net computer job growth over that period.[89] Critics also provide anecdotal evidence of visa holders working for less compensation.

If H-1B visa holders are needed to fill roles in the U.S. ICT industry as proponents claim, then the supposition is that the U.S. does not produce enough workers of its own. Companies and industry trade associations indeed believe a shortage of highly skilled ICT workers exists stemming from reduced interest in STEM careers, the loss of students at multiple points along the education pipeline, and poor math and science test scores. Their preferred solution is to increase the funding for and emphasis on STEM in primary, secondary, and post-secondary schools. As a stopgap measure until sufficient STEM grads are made available, companies and trade associations support increasing or eliminating annual visa caps to fill existing vacancies.

Others, however, question the existence of a shortage. A 2007 study found evidence of increases in the absolute numbers of secondary school graduates and increases in their math and science performance levels.[90] In addition, the authors discovered that the number of undergraduates completing degrees in science and engineering (S&E) has grown, the number of S&E graduates remains high by historical standards, and the number of qualified graduates far exceeds demand.[91] However, only one-third of such graduates end up in STEM careers; the others either accept employment in related fields, such as patent law, or completely different fields like finance and consulting. Moreover, the “best and the brightest” are more likely to move into non-STEM fields.

If indeed there are more graduates than job openings, why are companies unable to fill their vacancies with U.S. hires? The author’s of the above study note that some industries “may be voicing unrealistic expectations of experience more than skills or education of a new hire, or just cost….Managers in … technology firms do not claim a shortage of applicants nor do they complain of applicants with poor math and science skills or education. They do often note difficulty in finding workers with sufficient experience, specific technical skills, or a sufficient number of ‘brilliant’ workers in the pool.”[92] These assertions are consistent with what we have heard in our discussions with U.S. ICT companies, particularly the emphasis on experience and brilliance. Offshoring may also drive graduates away by signaling a lack of future U.S. growth.

Instead of a numerical shortage of workers, the ICT industry more likely confronts a mismatch between not only the skills available and demanded but also the need for experience largely unavailable to new college graduates. Global ICT companies now demand a workforce capable of operating in a variety of environments and are looking not just for a specific degree, but for broader skills such as communication, team building, collaboration, problem solving, and even cultural awareness, flexibility, willingness to travel, and languages.[93] It is in these areas that the education system fails to deliver. Companies are looking for well-rounded graduates, while schools continue to provide technically competent STEM graduates. For example, a 2011McKinsey study that found 40% of companies with plans to hire in the next 12 months had positions open for six months or longer because they couldn’t find the right candidate (right degree or experience); some of the most difficult to fill are in computer programming and IT.[94] The increasing time to fill rates echo a theme heard in our IS visits.

The human capital challenges in the ICT industry are magnified in DoD. In 2011, the DoD S&E workforce numbered 108,703, of which 36,788 worked in DoD labs.[95] The main challenge for the labs is the aging of its S&E workforce with a significant portion eligible for retirement beginning in the next few years and most out by 2020.[96] DoD faces unique challenges in recruiting a highly qualified STEM workforce to replace these workers. The main hurdles are the U.S. citizenship requirement (for classified work), the lengthy hiring process (including time required to receive a clearance), and the looming budget cuts. If new graduates believe no growth exists in the government sector or that the opportunity to solve challenging problems is in the private sector, they are unlikely to consider making DoD a career choice. At the same time, DoD needs its new STEM workforce to be flexible and easily adaptable to pursuing whatever technological challenges are required by a changing threat environment. [97] Similar constraints exist in the Defense Industrial Base. As of August 2011, DoD contractors were experiencing difficulty hiring systems engineers; some 800 positions remained open for more than 90 days.[98]

When it comes to PhDs, however, the number of eligible U.S. STEM grads declines and may become a barrier. Whereas 75% of all S&E bachelor's degrees are awarded to U.S. citizens, only 60% of the S&E PhDs go to Americans.[99] As that talent pool constricts, the demand for the services of the best and brightest will increase, along with the wages these individuals can command. Whether or not DoD can successfully compete at this level will be the determining factor in its ability to conduct world class basic and applied research in ICT technologies.
- Ms. Jill Christensen, Defense Intelligence Agency

Cyber Security: Cybersecurity is an enormous challenge requiring collaboration by all stakeholders but each must play its proper role. The Office of Management and Budget 2010 FISMA Report states that between 2009 and 2010 there was a 39% increase (41,776) in malicious cyber incidents on the federal network, and we know that number continues to increase. Symantec Corporation published that 50% of our critical infrastructure has been attacked and $114 billion is lost to cyber-crime annually around the world. Stuxnet, a highly specialized malware designed to target Siemens supervisory control and data acquisition systems, spread and infected numerous computers worldwide. It had a very target specific payload, reportedly impacting only Iran's uranium enrichment centrifuges causing them to spin out of control with no warning. Department of Energy and National Laboratory of Idaho researchers launched an experimental cyber-attack causing a generator to self-destruct. These two examples brought to life how cyber capabilities can generate kinetic effects with potentially devastating results. President Obama stated that "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation".[100] Government, industry, academia, and individuals at the national as well as international level have partnered to develop technical and non-technical solutions, to integrate strategic and tactical elements, and to grow professionals with the rights skills.

Government has created legislation and policy, such as the Federal Information Security Management Act of 2002 and the Cyber Security Policy of 2008; established the National Strategy to Secure Cyberspace with lead agencies for each of the major sectors of the economy vulnerable to infrastructure attack; stood up organizations such as the Department of Homeland Security to develop a comprehensive national cyber plan, the U.S. Cyber Command to protect U.S. military cyber capabilities, the FBI Cyber Division to investigate theft of information and online fraud, the Secret Service's Electronic Crimes Task Forces to investigate attacks on the nation's financial and critical infrastructure, and the Immigration and Customs Enforcement Cyber Crime Center to investigate money laundering and identity fraud; and funds education and research programs. Many government operations rely on commercial assets, to include Internet Service Providers and global supply chains, over which it has no direct authority. Working with the private sector requires a balance between regulation and volunteerism, as well incentives. Private sector's primary objective is to deliver value to its shareholders and naturally reluctant to accept regulatory measures. This situation is compounded for multinational companies operating under different legal and regulatory frameworks. Dependence on technology from untrusted sources and the increase in counterfeit products requires strong public-private sector cooperation.

The U.S. ICT industry works cooperatively with national, state, and local governments to improve cybersecurity. For example, the IT industry formed and funds the IT Sector Coordinating Council (IT-SCC) to work with DHS to ensure better preparedness and coordination of critical infrastructure initiatives and the IT Information Sharing and Analysis Center to exchange information among companies and DHS to identify, manage, and mitigate IT infrastructure risks. They are also involved in developing globally acceptable cybersecurity standards, best practices, and assurance programs. For example, they contribute to standards development through organizations such as the International Organization for Standardization, Organization for the Advancement of Structured Information Standards, and the Institute of Electrical and Electronics Engineers. The IT industry and government have been collaborating to develop risk management strategies and best practices, such as the National Infrastructure Protection Plan released by DHS to protect the nation's critical infrastructure and other key resources. Industry founded the National Cyber Security Alliance to provide education and awareness programs such as the "StopThinkConnect" campaign with DHS and the National Cyber Security Awareness Month in October to disseminate security messages.[101]

Some of the leading companies that specialize in cybersecurity products and services are Symantec, McAfee, Trend Micro, Entrust, and Comodo Group. Also, the trend has been for companies to purchase smaller security companies. For example, Hewlett-Packard purchased ArcSight, Symantec acquired Verisign, and Intel procured McAfee. One of the major problems is that cybersecurity practices lag behind technology. Solutions exist for many of the threats introduced by adversaries, but these solutions are not widely used because incentives are not aligned with objectives, resources are not correctly allocated, or people are not willing to follow policies. Some of the problems expressed by companies are insecure deployment of products, improper patching, excessive privileges, malicious insiders, improper network isolations of sensitive servers, and software vulnerabilities.

Securing our networks also depends on robust relationships with our allies and international partners. The U.S. government has bilateral critical infrastructure protection forums with trading partners including Japan and the E.U. Also, DHS conducts a biennial Cyber Storm exercise with federal, state, international and private sector participants to test and improve communications, policies, and procedures in response to cyber threats. President Obama signed the International Strategy for Cyberspace last year which calls for promoting international standards and norms, a shared understanding about acceptable behavior, and rule of law in cyberspace. Cyber security is a global issue and it is in our best interest to assist other countries in developing their own strategies - build secure technical capacity and specialized expertise, establish robust incident management, develop laws, and create a framework for sharing lessons learned. The Financial Action Task Force provides the technical tools and international cooperation framework to track and disrupt terrorist and cybercrime finance networks.[102] The Budapest Convention on Cybercrime "provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases."[103]

Although a daunting undertaking, much has been done to secure cyberspace and encourage norms of behavior. The U.S. government, ICT industry, research laboratories, and academia have invested a significant amount of effort into establishing a governance structure and developing solutions to the problem. All have collaborated to develop commercial products, cutting edge technology, standards, educational solutions, and cybersecurity capabilities. The next step should be the development of a more comprehensive cybersecurity plan defining a common set of standards as well as guidelines for assessing cyber preparedness. This includes a notification system to warn of infections and intrusions along with appropriate resources and tools to fix problems. Common standards for public and private sectors would ensure a base level of security. However, the standards must be industry-led while also including ideas from representatives of academia, and government. While DHS has been given significant authorities in this area, public and private firms have proven they are best equipped and motivated to ultimately solve the problem. Government must lead but it must also resist the urge to implement detailed, prescriptive legislative solutions which fail to keep up with the pace of technological change.
- Ms. Roxanna Zamora, Dept of the Air Force

Chapter X: Conclusion

The ICT industry is unquestionably healthy. Closer examination reveals this industry contributes significantly to U.S. GDP as well as increases in productivity and efficiency. It is also true that many of the most important innovations were achieved absent burdensome government regulation and oversight. As the pace of change quickens, it is doubtful that government policy makers will be able to keep pace. Government is no longer a dominant technology driver and in many areas firms do not even view government as a significant or valued customer.

Government policy makers do have a key role in the areas of stimulating, investing, and regulating. However, before undertaking additional policy debates leaders must come to the realization that the 20th century industrial age bureaucracy is not equipped to lead in this information age sector. Government must transform itself before it can effectively understand and regulate the ICT industry. Lessons learned at top firms in the areas of collaboration, productivity, security and energy efficiency would be a good first step. U.S. leaders should also pay careful attention China's expansion into emerging markets such as Africa.

While challenges do exist, the ICT industry has demonstrated real leadership in addressing shortcomings. With the proper amount of broad guidance, the ICT industry is capable of solving even the most important problems such as critical infrastructure protection and cybersecurity. Government policy makers should tread carefully and where politically possible, remove government regulation in favor of industry-developed standards.

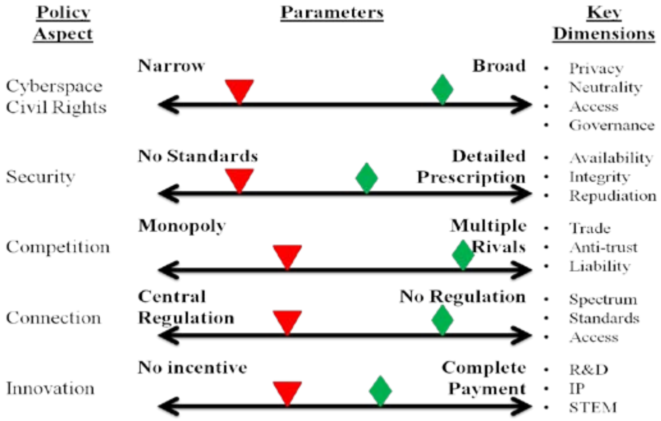
Appendix A – Guest Speakers and Lecturers

Throughout this study, the seminar benefited from the experience and expertise of numerous visitors from disparate sectors associated with the ICT industry. Some of these were guest lecturers who spoke to the entire ICAF student body. Most, however, were experts who agreed to speak to the ICT seminar to support specific topics associated with the study. We are extremely grateful to the individuals listed here for their willingness to speak with us and help in ensuring the thoroughness of this report.

Pierre Chao, Renaissance Strategic Advisors, LLC, Arlington, VA
Richard Clarke, AT&T
Chris Codella, PhD, IBM
Nicholas Fetchko, Telecommunications Industry Association (TIA)
Sheila Flynn, Department of State (Cyber)
Marc Forino, Department of State (Vietnam)
Amb. (Ret) David L. Gross, Wiley Rein LLP
John Kneuer, The John Kneuer Company LLC
Brett Lambo, DHS
Sara Litke, Department of State (Vietnam)
Mike McKeehan, Verizon
Mark Orndorff, DISA
Ronald Repasi, FCC
Steven Sinha, Department of State (China)
John Wecker, Department of State (China)
Tim Wyland, USTR
Elaine Wu, USPTO

Appendix B - ICT Policy Levers

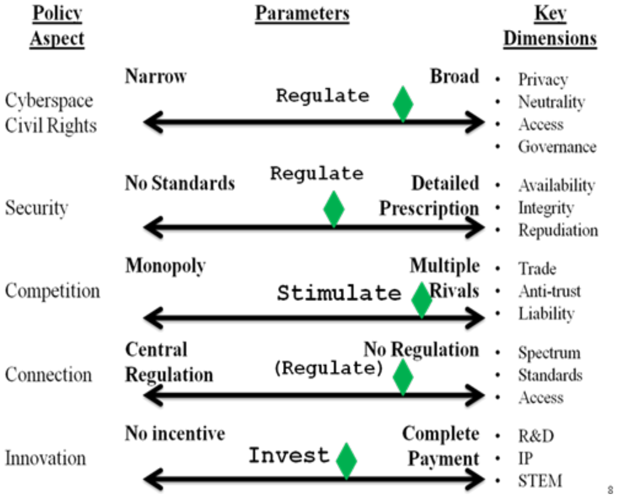
Figure 1: Policy Aspects and Key



Dimensions

▼ Current Policy ◆ Optimal Policy

Figure 2: Government's Role in Affecting Parameters



Appendix C – RF Spectrum Policy Alternative

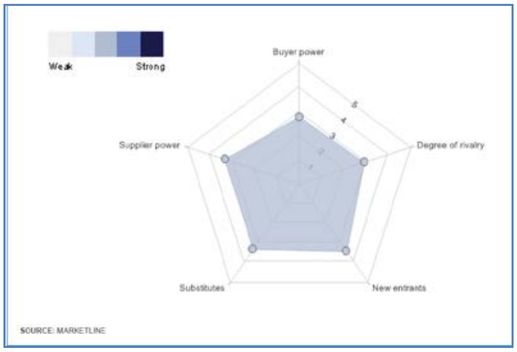
1. FCC/NTIA mandated auction of all spectrum, to include gov/emergency services [104]
2. Mandate the auction be voluntary. However, if a firm/entity does not put its spectrum up for bid then it cannot buy or sell additional spectrum for 5 years.[105]
3. No restrictions on who can bid for spectrum. Once a firm accepts a bid the proceeds go directly to that firm/gov entity in their entirety.[106]
4. No restrictions on usage of spectrum other than prohibitions on interference[107]
5. Current owners of spectrum do not have to accept any bids[108]
6. FCC/NTIA role is eliminated or reduced to enforcement only [109]

Realizing the political sensitivities as well as various industry and lobbying interests, several modifications to these proposed auction procedures are also recommended.

A. A small test-bed type auction be held in advance to determine initial lessons learned
B. Anti-trust provisions should also be included in the auction rules. This would stipulate the maximum amount of spectrum (both quantity and location) a single (or small number) of firms could own without an FCC waiver.
C. Provide for an eminent domain clause in the event a new technology operating in the best interest of the public requires previously allocated spectrum. An example could be the development of a medical, defense, or general research technology using a specific frequency when the benefits to the nation are disproportionately positive.
D. Some percentage of open access spectrum should be maintained.
E. Allow government agencies to keep spectrum revenue.

Appendix D – Porter's Five Forces[110]

The information communications technology industry is composed of numerous segments including computer hardware, software, information technology and internet access services, communications equipment and networking equipment. Each segment has unique attributes that differentiate one from another in each of Porter's Five Forces. For example, buyers in one segment do not necessarily equal buyers in another. Furthermore, the geopolitical and differences among various global economies act on market forces in the various industry segments. For this reason, a single overarching Five Forces analysis of the ICT industry is problematic. That said, solid conclusions on the health of the industry can still be drawn based on similarities and key differences among the various segments. Figures 3 is representative of the overall Five Forces industry analyses.



SOURCE: MARKETLINE

Figure 3. ICT Industry

Buyers in the computer hardware market are price sensitive and generally have low customer loyalty, thus increasing their power. Suppliers too have a strong position in being able to integrate forward and sell directly to consumers. A large threat to the personal computer market stems from gaming trends, as more gamers opt away from PC-based games to dedicated consoles, web-based and mobile device games.

In the area of internet access, buyers (end-users) have low switching costs and are unlikely to be loyal to a particular brand, increasing their power. However, this is a relatively untapped worldwide market, with a large number of potential buyers, and so this buyer power is diminished. This large pool also has a dampening effect upon industry rivalry as well. The suppliers to this market are the network owners and hardware/software manufactures, and their power is strong with a high cost of switching by the service providers. There are no real substitutes to internet access at this time.

The global communications market has been one of the few industries that continued to expand during the recent economic slowdowns, and is expected to be a major driver during the economic recovery. The great diversity of communications equipment gives the buyers a great deal of choice, however as mentioned previously, the vast number of potential buyers, with their relatively small financial ability, lowers the buyer power. This condition also increases the potential of new entrants.

The buyers of networking equipment are end-users, both individual and businesses, and the suppliers are the manufacturers of such equipment. In contrast to the other ICT segments, the degree of rivalry is relatively higher in this segment as there are higher fixed costs and lower switching costs for buyers. Security, quality and reliability are key differentiators of networking equipment. Buyer power is relatively greater in this segment since it contains large institutions with greater financial resources to purchase large amounts of networking hardware and services, with low switching costs. Some companies in this industry are integrating vertically, which decreases supplier power.

The software industry has a strong effect on the ICT industry as an enabler for providing services accessed via ICT equipment. Switching costs can be high, for example, if a company is wedded to a particular brand of enterprise software or operating system. However, interoperability among various players is increasing. Supplier power is high if one considers skilled programmers as a supply item. Their scarcity drives high salaries and decreased loyalty to any particular company. Some companies mitigate this by providing additional training on their particular software (and hardware), making the programmers more valuable still. The threat of substitutes is strong due to the availability of free, open source software with the same basic utility as purchased or licensed software.

Appendix E – Definition of Terms

ACTA: Anti-Counterfeiting Trade Agreement

AIA: America Invents Act

BTOP: Broadband Technology Opportunities Program

CIKR: Critical Infrastructure and Key Resources

DHS: Department of Homeland Security

DNS: Domain Name System

DoD: Department of Defense

DOE: Department of Energy

DOS: Department of State

DNS: Domain Name System

FCC: Federal Communications Commission

FISMA: Federal Information Security Management Act

GAO: Government Accountability Office

GDP: Gross Domestic Product

IC: Intelligence Community

ICT: Information Communications Technology

IPEC: Intellectual Property Enforcement Coordinator

IP: Intellectual Property (or Internet Protocol)

IT: Information Technology

IT-SCC: IT Sector Coordinating Council

ISP: Internet Service Provider

ITU: International Telecommunication Union

LTE: Long Term Evolution

MPLS: Multi Protocol Label Switching

NASA: National Aeronautics and Space Administration

NBP: National Broadband Plan

NTIA: National Telecommunications and Information Administration

OECD: Organization for Economic Cooperation and Development

R&D: Research and Development

RF: Radio Frequency

STEM: Science Technology Engineering and Math

TRIPS: Trade-Related Aspects of Intellectual Property Rights

VPN: Virtual Private Networks

VoIP: Voice over Internet Protocols

WTO: World Trade Organization

[1] Central Intelligence Agency (CIA). "CIA – The World Fact Book: United States." https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (accessed March 19, 2012).

[2] Robert J. Shapiro and Aparna Mathur, "The Contributions of Information and Communication Technologies to American Growth, Productivity, Jobs and Prosperity." September 2011: 4.

[3] Ibid., 3-4.

[4] Ibid., 3.

[5] Ibid., 6.

[6] Ibid., 20.

[7] Ibid., 21.

[8] Kenneth Rapoza. "Bringing Overseas Corporate Profits Back to US Not Necessarily a Job Booster." Forbes, September 9, 2011. http://www.forbes.com/sites/kenrapoza/2011/09/12/bringing-overseas-corporate-profits-back-to-us-not-necessarily-a-job-booster/ (accessed March 6, 2012).

[8]David Kocieniewski. "Companies Push for Tax Break on Foreign Cash." The New York Times, June 19, 2011. http://www.nytimes.com/2011/06/20/business/20tax.html?pagewanted=all (accessed March 6, 2012).

[9] "Sales Tax on the Internet." http://www.nolo.com/legal-encyclopedia/sales-tax-internet-29919.html (accessed April 13, 2012).

[10] "Internet Sales Tax Fairness." Institute for Local Self Reliance Web Site. http://www.ilsr.org/rule/internet-sales-tax-fairness/ (accessed April 13, 2012).

[11] "Morning Bell: The Internet Taxes that Could Be Coming." The Foundry: Conservative Policy News Blog from the Heritage Foundation. http://blog.heritage.org/2012/04/12/morning-bell-the-internet-taxes-that-could-be-coming/ (accessed April 13, 2012).

[12] Presidential Commission, *Presidential Commission on Critical Infrastructure Protection Report,* Washington, D.C.,1997

[13] Department of Homeland Security, 2009

[14] Faulhaber, Gerald R, and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

[15] IBISWorld Industry Reports 51711a-e. http://clients.ibisworld.com/search/default.aspx?st=51711&srtid=1 (accessed 1 Mar 2012).

[16] Joseph C. Andersen & Danielle Coffey, "TIA Innovation White Paper: U.S. ICT R&D Policy Report," .Telecommunications Industry Association, http://www.tiaonline.org/gov_affairs/fcc_filings/documents/TIA_US_ICT_R&D_Policy_Report.pdf (accessed March 1, 2012) 1.

[17] Congressional Research Service, *International Trade and Finance: Key Policy Issues for the 112th Congress, 2nd Session*," (Washington, DC: Congressional Research Service, February 8, 2012), 22.

[18]George H. Pike, "The Next Step in Patent Reform," *Information Today*, Vol 28 (10), November 2011: 33-34. In 1990, the USPTO received 164,558 patent applications. In 2000, this number grew to 295,926. By 2010, the number of applications exploded to 490,226 and the USPTO had a backlog of over 700,000 applications pending.

[19] E. Robert Yoches, Esther H. Lim, Christopher S. Schultz, Linda J. Thayer, Erika H. Arner, and Rebecca M. McNeill, "How Will Patent Reform Affect the Software and Internet Industries?" *Computer and Internet Lawyer,* Vol 28 (12), December 2011, 5.

[20] George H. Pike, "The Next Step in Patent Reform,": 33-34

[21] Barack Obama, *National Security Strategy*, (Washington, D.C.: The White House, May 2010), 27.

[22] National Academy of Sciences, *Rising Above the Gathering Storm, Energizing and Employing America for a Brighter Economic Future,* (Washington D.C.: The National Academy Press, 2006).

[23] Web 1 was a broadcast medium. Web 2 is an interactive medium. The evolution of the Web is the shift from an information based platform to a relationship based platform. This is not only the relationship between humans but also the relationship between humans and machines and between multiple sources of information. As a metaphor, web 1 was about the leopard's spots, web 2 is about the tessellations.

[24] Carafano, James Jay. "Social Networking and National Security: How to Harness Web 2.0 to Protect the Country." *FamilySecurity Matters.org.* May 21, 2009. http://www.familysecuritymatters.org/publications/id.3296/pub_detail.asp (accessed March 7, 2012).

[25] International visits revealed the power of social networks to dramatically impact dialogue and diplomatic relationships at all levels. Subtle communication of images such as an ambassador buying coffee and carrying his own luggage and the accessibility of President Obama (as show through images with ordinary citizens wearing jeans) were extremely powerful in China and Hong Kong. Even the communication of air quality information is proving to be a powerful tool in building trust with typical Chinese citizens.

[26] According to the FCC, high-speed wireline Internet connections have flattened. Growth in the first half of 2010 was 1 percent, totaling 82 million connections. Meanwhile, mobile broadband connections in the same period grew by more than 27 percent to more than 71 million connections.

Data taken from -- Verizon Communications Corporate Webpage, “Investor Relations, Company Info, Company Profile, Industry Overview,” http://www22.verizon.com/investor/industryoverview.htm (accessed 10 Mar 2012)

[27] *Rising Above the Gathering Storm, Energizing and Employing America for a Brighter Economic Future*. 208.

[28] E. H. Preeg, *The Emerging Chinese Advanced Technology Superstate.* (Arlington, VA: Manufacturers Alliance/MAPI and Hudson Institute, 2005); K. Walsh, *Foreign High-Tech R&D in China: Risks, Rewards, and Implications for US-China Relations, (*Washington, DC: Henry L. Stimson Center, 2003)

[29] Daniel Thomas and Paul Taylor, “Huawei lets loose its technological ambition,” Financial Times, February 29, 2012, http://www.ft.com/cms/s/0/208bbd58-62f3-11e1-b837-00144feabdc0.html (accessed March 1, 2012).

[30] Oracle Corporation Annual Report (SEC 10K Filing), filed June 28, 2011.

[31] “China to inch past U.S. as largest smartphone market in 2012,” Posted March 15, 2012 http://www.fiercemobilecontent.com/press-releases/china-become-largest-market-smartphones-2012-brazil-and-india-forecast-join (accessed March 16, 2012).

[32] Robert J. Shapiro and Aparna Mathur, *The Contribution of ICT to American Growth, Productivity, Jobs, and Prosperity*, (September 2011), 1. http://tiaonline.org/gov_affairs/fcc_filings/documents/Report_on_ICT_and_Innovation_Shapiro_Mathur_September_8_2011.pdf (accessed 10 Mar 2012).

[33] Organization for Economic Cooperation and Development, *Developments in Fibre Technologies and Investment*, (Apr 2008), 5. http://search.proquest.com.ezproxy6.ndu.edu/docview/874154111/13586C4568A4C9C8B1B/1?accountid=12686 (accessed 27 Feb 2012).

[34] Nicole Gaouette and Brendan Greeley, "U.S. Funds Help Democracy Activists Evade Internet Crackdowns," Bloomberg News, April 20, 2011, http://www.bloomberg.com/news/2011-04-20/u-s-funds-help-democracy-activists-evade-internet-crackdowns.html (accessed March 18, 2012).

[35] Patricia Moloney Figliola, Angele A. Gilroy and Lennard G. Kruger, “The Evolving Broadband Infrastrucutre: Expansion, Application, and Regulation,” *Congressional Research Service Report*, (February 19, 2009), i. http://web.lexis-nexis.com.ezproxy6.ndu.edu/congcomp/attachment/a.pdf?_m=5aac4a1d07d998cd5a6746b6188ca3ff&wchp=dGLzVzS-zSkSA&_md5=bf5c33a373c60e0a055db5de983faca0&ie=a.pdf (accessed 28 Feb 2012).

[36] Faulhaber, Gerald R, and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

[37] Wylie Wong, "FedTech Case Studies,” FedTech Magazine, http://www.fedtechmagazine.com /article/2011/08/dynamics-cloud-security, 20 March 2012

[38] *American Recovery and Reinvestment Act of 2009*, Public Law 111-5, 111th Congress (February 17, 2009), 516.

[39] “The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost.” *Federal Communications Commission*. (June 2010): 3.

[40] Ibid., xiv-xv.

[41] Michael J. Copps. “Bringing Broadband to Rural America: Report on a Rural Broadband Strategy.” *Federal Communications Commission*. (2009): 1.

[42] Ibid., 24-25.

[43] Ibid., 24-25.

[44] “Connecting America: The National Broadband Plan.” *Federal Communications Commission*, (2010): 333-334.

[45] Ibid., 75.

[46] Ibid., 75.

[47] *Middle Class Tax Relief and Job Creation Act of 2012*. (Public Law H.R. 3630, 112th Congress, 2nd Session. (2012): 46.

[48] Ibid., 2-3.

[49] Ibid., 50.

[50] Ibid., 50.

[51] Ibid., 57.

[52] Ibid., 53-54.

[53] Ibid., 76.

[54] Ibid., 79.

[55] “Report and Order FCC 10-201: Preserving the Open Internet and Broadband Industry Practices.” *Federal Communications Commission*. (December 21, 2010): 2.

[56] Ibid., 2.

[57] Ibid., 2.

[58] Ibid., 2.

[59] Ibid., 5.

[60] Ibid., 5.

[61] Angela A. Gilroy. “Access to Broadband Networks: The Net Neutrality Debate.” *Congressional Research Service.* (October 25, 2011): 3.

[62] Ibid., 3.

[63] Ibid., 3.

[64] Ibid., 3.

[65] Josh Smith. “Wireless Association Joins Net Neutrality Lawsuit.” NationalJournal Daily. (2012): http://techdailydose.nationaljournal.com/2011/10/wireless-association-joins-net.php.

[66] Angela A. Gilroy. “Access to Broadband Networks: The Net Neutrality Debate.” Congressional Research Service. (October 25, 2011): 5-6.

[67] Cindy Cohn. “A Review of Verizon and Google’s Net Neutrality Proposal.” *Electronic Frontier Foundation.* (August 10, 2012): 1. https://www.eff.org/deeplinks/2010/08/google-verizon-netneutrality.

[68] Ibid., 1.

[69] http://www.broadband.gov/plan/

[70] "QuickMBA Strategic Management." http://www.quickmba.com/strategy/porter.shtml (accessed Mar 14, 2012).

[71] "CITA The Wireless Association." *Spectrum, Tower Siting & Antennas.* http://files.ctia.org/pdf/101810_-_Spectrum.pdf (accessed Mar 15, 2012).

[72] "IBISWorld." *IBISWorld Industry Report 51332 Wireless Telecommunications Carriers in the US.* http://clients.ibisworld.com/industryus/default.aspx?indid=1267 (accessed Mar 15, 2012).

[73] Faulhaber, Gerald R, and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

[74] Ibid.

[75] Partridge, Craig. "Realizing the Future of Wireless Data Communications." *Communications of the ACM*, Sep 2011.

[76] Coase, Ronald A. *Autobiography of Ronald Coase, Nobel Laureate.* 1991. http://www.nobelprize.org/nobel_prizes/economics/laureates/1991/coase-autobio.html (accessed Mar 15, 2012).

[77] Anna-Maria Kovacs, Ph.D., CFA. *Neutral Spectrum Auctions: Maximizing Proceeds and Consumer Benefit.* Economic Policy Vignette, Washington DC: Georgetown University Center for Businsess and Public Policy, 2012.

[78] Ibid.

[79] International Telecommunication Union. *Beyond Licenced vs. Unlicenced: Spectrum Access Rights Continua.* Geneva: ITU, 2007.

[80] Faulhaber, Gerald R, and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

[81] Ibid.

[82] Lindsay B. Lowell and Hal Salzman,”Into the Eye of the Storm: Assessing the Evidence on Science and Engineering Education, Quality, and Workforce Demand,” The Urban Institute, October 2007, 36.

[83] Patrick Thibodeau, “GAO, DOJ seek H-1B visa reforms,” *ComputerWorld* online, January 14, 2011 (accessed March 18, 2012).

[84] “Characteristics of H-1B Specialty Occupation Workers: Fiscal Year 2010 Annual Report October 1, 2009-September 30, 2010,” U.S. Citizenship and Immigration Services (USCIS), August 4, 2011,5.

[85] Patrick Thibodeau, “Senate’s H-1B foes begin new attack,” *ComputerWorld* online, February 1, 2011. Regarding F-1s, A 2008 decision extended F-1 student visas for STEM graduates from one year to 29 months, meaning at least some of the graduates who otherwise might have been candidates for an H-1B were able to work in STEM fields for an additional 17 months before needing to transition to an H-1B. Information on F-1s and the OPT extension can be found on the USCIS website (www.uscis.gov).

[86] Patrick Thibodeau, “Top H-1B visa user of 2010: An Indian Firm,” *ComputerWorld* online, February 11, 2011 (accessed March 12, 2012). Others at the top included offshoring company Cognizant Technology Solutions, Microsoft, Wipro Limited, IBM India, Accenture, Larsen & Toubro Infotech, Satyam Computer Services, Mphasis Corporation, Deloitte Consulting, Google, and Patni America.

[87] USCIS FY 2010 H-1B Annual Report,5

[88] Ibid.,9,10,12,16,20.

[89] Ibid.

[90] Lowell and Salzman,”Into the Eye of the Storm”,ii.

[91] Ibid.

[92] Lowell and Salzman,”Into the Eye of the Storm,”36.

[93] Lynn and Salzman, “The Real Global Technology Challenge,”13.

[94] James Manyika, Susan Lund, Byron Auguste, Lenny Mendonca, Tim Welsh, and Sreenivas Ramaswamy, “An economy that works: Job creation and America’s future,” McKinsey Global Institute, June 2011, 16, 41, 78.

[95] Lowell and Salzman, “Into the Eye of the Storm,” 22.

[96] Jocelyn M Seng and Pamela Flattau, “Assessment of the DoD Laboratory Civilian Science and Engineering Workforce,” Institute for Defense Analysis, (June 2009), ES-4.

[97] Participants in the August 2011 National Academy of Sciences workshop of the Committee on Science, Technology, Engineering, and, Mathematics (STEM) Workforce Needs for the U.S. Department of Defense and the U.S. Defense Industrial Base discussed at length the issues associated with recruiting and retaining the right STEM graduates.

[98] “Report of a Workshop on STEM Workforce Needs for DoD and the DIB,” 4.

[99] These numbers are derived from National Science Foundation data presented on p.8 of the “Report of a Workshop on STEM Workforce Needs for DoD and the DIB.

[100] Barack Obama, *National Security Strategy,* (Washington, D.C.: The White House, May 2010), 27.

[101] *The IT Industry’s Cybersecurity Principles for Industry and Government,* (Washington, D.C.: Information Technology Industry Council, 2011), 10-20.

[102] Barack Obama, *International Strategy for Cyberspace*, (Washington, D.C.: The White House, 2011), 11.

[103] Ibid., p. 20.

[104] Faulhaber, Gerald R, and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

[105] Ibid.

[106] Ibid.

[107] Ibid.

[108] Ibid.

[109] Ibid.

[110] Compilation of analysis from *Marketline Industry Profiles*. Retrieved May 15, 2012, from http://www.marketlineinfo.com/library/DisplayContent.aspx?N=210

Bibliography

American Recovery and Reinvestment Act of 2009, Public Law 111-5, 111th Congress (February 17, 2009).

Angela A. Gilroy. "Access to Broadband Networks: The Net Neutrality Debate." *Congressional Research Service.* (October 25, 2011): 3.

Anna-Maria Kovacs, Ph.D., CFA. *Neutral Spectrum Auctions: Maximizing Proceeds and Consumer Benefit.* Economic Policy Vignette, Washington DC: Georgetown University Center for Businsess and Public Policy, 2012.

Barack Obama. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," Washington, D.C.: The White House, (May 2011): 11.

Barack Obama. "The National Security Strategy." May 2010. www.whitehouse.gov/sites/default/.../national_security_strategy.pdf (accessed Dec 2, 2011).

"Broadband.gov." *Federal Communications Commission.* http://www.broadband.gov/plan/ (accessed Mar 14, 2012).

Central Intelligence Agency (CIA). "CIA – The World Fact Book: United States." https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (accessed March 19, 2012).

"Characteristics of H-1B Specialty Occupation Workers: Fiscal Year 2010 Annual Report October 1, 2009-September 30, 2010." U.S. Citizenship and Immigration Services, Department of Homeland Security. August 4, 2011.

"China to inch past U.S. as largest smartphone market in 2012," Posted March 15, 2012 HYPERLINK "http://www.fiercemobilecontent.com/press-releases/china-become-largest-market-smartphones-2012-brazil-and-india-forecast-join" http://www.fiercemobilecontent.com/press-releases/china-become-largest-market-smartphones-2012-brazil-and-india-forecast-join (accessed March 16, 2012).

Cindy Cohn. "A Review of Verizon and Google's Net Neutrality Proposal." *Electronic Frontier Foundation*. (August 10, 2012): 1. https://www.eff.org/deeplinks/2010/08/google-verizon-netneutrality.

"CITA The Wireless Association." *Spectrum, Tower Siting & Antennas.* http://files.ctia.org/pdf/101810_-_Spectrum.pdf (accessed Mar 15, 2012).

Coase, Ronald A. *Autobiography of Ronald Coase, Nobel Laureate.* 1991. http://www.nobelprize.org/nobel_prizes/economics/laureates/1991/coase-autobio.html (accessed Mar 15, 2012).

Congressional Research Service, *International Trade and Finance: Key Policy Issues for the 112th Congress, 2nd Session*," (Washington, DC: Congressional Research Service, February 8, 2012).

David Kocieniewski. "Companies Push for Tax Break on Foreign Cash." The New York Times, June 19, 2011. HYPERLINK "http://www.nytimes.com/2011/06/20/business/20tax.html?pagewanted=all" http://www.nytimes.com/2011/06/20/business/20tax.html?pagewanted=all (accessed March 6, 2012).

Daniel Thomas and Paul Taylor, "Huawei lets loose its technological ambition," Financial Times, February 29, 2012, HYPERLINK "http://www.ft.com/cms/s/0/208bbd58-62f3-11e1-b837-00144feabdc0.html" http://www.ft.com/cms/s/0/208bbd58-62f3-11e1-b837-00144feabdc0.html (accessed March 1, 2012).

"Department of Defense Strategy for Operating in Cyberspace," Washington, D.C.: U.S. Government Printing Office, (July 2011): 1.

Department of Homeland Security. "DHS Announces AT&T PS Prep Certification." *Press Release.* Washington, DC, March 14, 2012.

Department of Homeland Security. "National Infrastructure Protection Program." 2009.

Department of Homeland Security. *National Strategy for Homeland Security.* Strategy, Washington, DC: US Government, 2002.

E. H. Preeg, *The Emerging Chinese Advanced Technology Superstate.* (Arlington, VA: Manufacturers Alliance/MAPI and Hudson Institute, 2005); K. Walsh, *Foreign High-Tech R&D in China: Risks, Rewards, and Implications for US-China Relations, (*Washington, DC: Henry L. Stimson Center, 2003)

E. Robert Yoches, Esther H. Lim, Christopher S. Schultz, Linda J. Thayer, Erika H. Arner, and Rebecca M. McNeill, "How Will Patent Reform Affect the Software and Internet Industries?" *Computer and Internet Lawyer*, Vol 28 (12), December 2011, 5.

Gerald R. and David Farber. *Spectrum Management: Property Rights, Markets and the Commons.*

George H. Pike, "How Far is too Far: The SOPA Debate," *Information Today*, Vol 27 (1), January 2012: 24.

George H. Pike, "The Next Step in Patent Reform," *Information Today*, Vol 28 (10), November 2011: 1.

"IBISWorld." *IBISWorld Industry Report 51332 Wireless Telecommunications Carriers in the US.* http://clients.ibisworld.com/industryus/default.aspx?indid=1267 (accessed Mar 15, 2012).

"IBISWorld." Industry Reports 51711a-e. HYPERLINK "http://clients.ibisworld.com/search/default.aspx?st=51711&srtid=1" http://clients.ibisworld.com/search/default.aspx?st=51711&srtid=1 (accessed 1 Mar 2012).

International Telecommunication Union. *Beyond Licenced vs. Unlicenced: Spectrum Access Rights Continua.* Geneva: ITU, 2007.

“Internet Sales Tax Fairness.” Institute for Local Self Reliance Web Site. HYPERLINK "http://www.ilsr.org/rule/internet-sales-tax-fairness/" http://www.ilsr.org/rule/internet-sales-tax-fairness/ (accessed April 13, 2012).

James Jay Carafano, Ph.D. "WebMemo." *The Heritage Foundation.* June 9, 2011. http://report.heritage.org/wm3286 (accessed June 9, 2011).

James Jay Carafano. "Social Networking and National Security: How to Harness Web 2.0 to Protect the Country." *FamilySecurity Matters.org.* May 21, 2009. http://www.familysecuritymatters.org/publications/id.3296/pub_detail.asp (accessed March 7, 2012).

James Manyika, Susan Lund, Byron Auguste, Lenny Mendonca, Tim Welsh, and Sreenivas Ramaswamy, “An economy that works: Job creation and America’s future,” McKinsey Global Institute, June 2011.

Joseph C. Andersen & Danielle Coffey, "TIA Innovation White Paper: U.S. ICT R&D Policy Report," .Telecommunications Industry Association, HYPERLINK "http://www.tiaonline.org/gov_affairs/fcc_filings/documents/TIA_US_ICT_R&D_Policy_Report.pdf" http://www.tiaonline.org/gov_affairs/fcc_filings/documents/TIA_US_ICT_R&D_Policy_Report.pdf (accessed March 1, 2012) 1.

Josh Smith. “Wireless Association Joins Net Neutrality Lawsuit.” NationalJournal Daily. (2012): http://techdailydose.nationaljournal.com/2011/10/wireless-association-joins-net.php.

Kenneth Rapoza. “Bringing Overseas Corporate Profits Back to US Not Necessarily a Job Booster.” Forbes, September 9, 2011. HYPERLINK "http://www.forbes.com/sites/kenrapoza/2011/09/12/bringing-overseas-corporate-profits-back-to-us-not-necessarily-a-job-booster/" http://www.forbes.com/sites/kenrapoza/2011/09/12/bringing-overseas-corporate-profits-back-to-us-not-necessarily-a-job-booster/ (accessed March 6, 2012).

Laura Tyson and Greg Linden.” The Corporate R&D Tax Credit and U.S. Innovation and Competitiveness: Gauging the Economic and Fiscal Effectiveness of the Credit.” Center for American Progress, January 2012. HYPERLINK "http://www.americanprogress.org/issues/2012/01/pdf/corporate_r_and_d.pdf" http://www.americanprogress.org/issues/2012/01/pdf/corporate_r_and_d.pdf (accessed March 12, 2012): 35.

Lindsay B. Lowell. and Hal Salzman. “Into the Eye of the Storm: Assessing the Evidence on Science and Engineering Education, Quality, and Workforce Demand.” The Urban Institute. October 2007.

Lynn, Leonard and Harold Salzman. “The Real Global Technology Challenge.” *Change: Magazine of Higher Learning.* July/August 2007.

Mashable. http://mashable.com/follow/videos/1466179506001-a-report-from-analysis-firm-ovum-concluded-mobile-carriers-lost-nea (accessed Mar 15, 2012).

Marketline Industry Profiles. Retrieved May 15, 2012, from HYPERLINK "http://www.marketlineinfo.com/library/DisplayContent.aspx?N=210" http://www.marketlineinfo.com/library/DisplayContent.aspx?N=210

Michael J. Copps. "Bringing Broadband to Rural America: Report on a Rural Broadband Strategy." *Federal Communications Commission*. (2009): 1.

Middle Class Tax Relief and Job Creation Act of 2012. (Public Law H.R. 3630, 112th Congress, 2nd Session. (2012): 46.

"Morning Bell: The Internet Taxes that Could Be Coming." The Foundry: Conservative Policy News Blog from the Heritage Foundation. HYPERLINK "http://blog.heritage.org/2012/04/12/morning-bell-the-internet-taxes-that-could-be-coming/" http://blog.heritage.org/2012/04/12/morning-bell-the-internet-taxes-that-could-be-coming/ (accessed April 13, 2012).

Murphy, Chris. *Information Week Global CIO*. Jan 25, 2010. http://www.informationweek.com/news/global-cio/security/222500027 (accessed Mar 15, 2012).

National Academy of Sciences, *Rising Above the Gathering Storm, Energizing and Employing America for a Brighter Economic Future*, (Washington D.C.: The National Academy Press, 2006).

Nicole Gaouette and Brendan Greeley, "U.S. Funds Help Democracy Activists Evade Internet Crackdowns," Bloomberg News, April 20, 2011, http://www.bloomberg.com/news/2011-04-20/u-s-funds-help-democracy-activists-evade-internet-crackdowns.html (accessed March 18, 2012).

Noam, Eli. *Beyond Auctions: Open Spectrum Access*. Columbia University.

Oracle Corporation Annual Report (SEC 10K Filing), filed June 28, 2011.

Organization for Economic Cooperation and Development, *Developments in Fibre Technologies and Investment*, (Apr 2008), 5. HYPERLINK "http://search.proquest.com.ezproxy6.ndu.edu/docview/874154111/13586C4568A4C9C8B1B/1?accountid=12686" http://search.proquest.com.ezproxy6.ndu.edu/docview/874154111/13586C4568A4C9C8B1B/1?accountid=12686 (accessed 27 Feb 2012).

Partridge, Craig. "Realizing the Future of Wireless Data Communications." *Communications of the ACM*, Sep 2011.

Patricia Moloney Figliola, Angele A. Gilroy and Lennard G. Kruger, "The Evolving Broadband Infrastrucutre: Expansion, Application, and Regulation," *Congressional Research Service Report*, (February 19, 2009), i. HYPERLINK "http://web.lexis-nexis.com.ezproxy6.ndu.edu/congcomp/attachment/a.pdf?_m=5aac4a1d07d998cd5a6746b6188ca3ff&wchp=dGLzVzS-zSkSA&_md5=bf5c33a373c60e0a055db5de983faca0&ie=a.pdf"

http://web.lexis-nexis.com.ezproxy6.ndu.edu/congcomp/attachment/a.pdf?_m=5aac4a1d07d998cd5a6746b6188ca3ff&wchp=dGLzVzS-zSkSA&_md5=bf5c33a373c60e0a055db5de983faca0&ie=a.pdf (accessed 28 Feb 2012).

Presidential Commission. *President's Commission on Critical Infrastructure Protection Report.* Commission, Washington, DC: Whithouse, 1997.

"QuickMBA Strategic Management." http://www.quickmba.com/strategy/porter.shtml (accessed Mar 14, 2012).

“Report and Order FCC 10-201: Preserving the Open Internet and Broadband Industry Practices.” *Federal Communications Commission.* (December 21, 2010): 2.

“Report on H-1B Petitions: Fiscal Year 2010 Annual Report October 1, 2009-September 30, 2010.” U.S. Citizenship and Immigration Services, Department of Homeland Security. August 4, 2011.

“Report of a Workshop on Science, Technology, Engineering, and Mathematics (STEM) Workforce Needs for the U.S. Department of Defense and the U.S. Defense Industrial Base.” The Committee on Science, Technology, Engineering, and Mathematics (STEM) Workforce Needs for the U.S. Department of Defense and the U.S. Defense Industrial Base. Washington, DC: National Academies Press, 2012.

“Sales Tax on the Internet.” `HYPERLINK "http://www.nolo.com/legal-encyclopedia/sales-tax-internet-29919.html"` http://www.nolo.com/legal-encyclopedia/sales-tax-internet-29919.html (accessed April 13, 2012).

Shapiro, Robert J., and Aparna Mathur. "The Contributions of Information and Communications Technologies to American Growth, Productivity, Jobs and Prosperity." September 2011.

Seng, Jocelyn M. and Pamela Ebert Flattau. “Assessment of the DoD Laboratory Civilian Science and Engineering Workforce.” Institute for Defense Analysis. IDA Paper P-4469. June 2009. (Accessed March 17, 2012.)

TIA Whitepaper. “Broadband Spectrum: The Engine for Innovation, Job Growth, and Advancement of Social Priorities.” March 2011: 2. http://www.tiaonline.org/sites/default/files/pages/TIASpectrumWhitePaperFINAL.pdf (accessed March 15, 2012).

“The IT Industry’s Cybersecurity Principles for Industry and Government,” Washington, D.C.: Information Technology Industry Council, (2011): 10-20.

“The Public Safety Nationwide Interoperable Broadband Network: A New Model for Capacity, Performance and Cost.” *Federal Communications Commission*. (June 2010): 3.

Thibodeau, Patrick. “Senate’s H-1B foes begin new attack.” *ComputerWorld* online. February 1, 2011. (Accessed March 18, 2012).

Thibodeau, ___. “GAO, DOJ seek H-1B visa reforms.” *ComputerWorld* online. January 14, 2011. (Accessed March 18, 2012).

Thibodeau, ___. “Top H-1B visa user of 2010: An Indian Firm.” *ComputerWorld* online. February 11, 2011. (Accessed March 12, 2012).

Thibodeau, ___. “H-1B workers are better paid, more educated, study finds.” *Computer World* online. February 3, 2012. (Accessed March 17, 2012).

Thibodeau, ___. “Engineer’s wife ‘ferocious’ in Obama Q&A on H-1Bs.” *Computer World* online. February 3, 2012. (Accessed March 17, 2012).

Verizon Communications Corporate Webpage, “Investor Relations, Company Info, Company Profile, Industry Overview,” HYPERLINK "http://www22.verizon.com/investor/industryoverview.htm" http://www22.verizon.com/investor/industryoverview.htm (accessed 10 Mar 2012)

Wylie Wong, "FedTech Case Studies,” FedTech Magazine, http://www.fedtechmagazine.com /article/2011/08/dynamics-cloud-security, 20 March 2012