Spring 2011
Industry Study

Final Report
Information and Communications Technology Industry

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

INFORMATION & COMMUNICATIONS TECHNOLOGY INDUSTRY REPORT

ABSTRACT: The Information and Communications Technology (ICT) industry enables connectedness that is improving the quality of life for millions of people while promoting increased productivity worldwide. The U.S. ICT industry continues to lead the world in innovation and available capital but is experiencing increasing challenges from global ICT firms. Value creation, commoditization, capacity limitations, and cybersecurity issues dynamically test the market fundamentals of the ICT industry. The convergence of ICT capabilities and demand for mobile capacity are now driving many economic, legislative, and technological trends. The U.S. government must pursue policies that promote innovation, modernization, and cybersecurity to maintain global ICT leadership, improve our standard of living, and promote our national security. 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 James Bell, U.S. Air Force
Colonel Lance Bunch, U.S. Air Force
Captain Ron Florence, U.S. Navy
Colonel Mathieu Fossat, French Ministry of Defense
Mr. James Gough, Dept of the Navy
Colonel Patricia Ham, U.S. Army
Lieutenant Colonel Kimberlee Joos, U.S. Air Force
Commander Blaine Lorimer, U.S. Navy
Colonel Trond Lundberg, Norwegian Army
Colonel John McLaughlin, U.S. Army
Mr. Frank Myers, Office of the Secretary of Defense
Mr. Christopher Pinzino, Dept of State
Commander George Segredo, U.S. Navy
Mr. Peter Vrooman, Dept of State
Colonel Clifford Wheeler, U.S. Army
Mr. James White, Harris Corporation

Colonel David King, Canadian Forces (Retired), Faculty Lead
Colonel Richard Altieri, J.D., U.S. Army (Retired), Faculty
Colonel Lynne Thompson, EdD, U.S. Air Force (Retired), Faculty

PLACES VISITED

Domestic:

AT&T (Washington, DC)
Brocade Communications (San Jose, CA)
Cisco Systems (San Jose, CA)
CollabWorks, Computer History Museum (Mountain View, 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)
Oracle (Redwood City, CA)
SAP (Palo Alto, CA)
Software and Information Industry Association (SIIA) (Washington, DC)
Sprint (Reston, VA)
TechAmerica (Washington, DC)

International:

American Chamber of Commerce (AMCHAM), Hong Kong
American Chamber of Commerce in Vietnam (AMCHAM), Ho Chi Minh City, Vietnam
Baidu, Beijing, China
China Academy of Telecommunications Research (CATR), Beijing, China
China Mobile, Guangzhou, China
China Unicom, Beijing, China
Cisco, Guangzhou, China
City Telecom, Hong Kong, China
CSL Cyberport, Hong Kong, China
Department of Information and Communication, Ho Chi Minh City, Vietnam
Duncan Clarke, BDA, Beijing, China
Intel, Saigon Hi-Tech Park, Ho Chi Minh City, Vietnam
EVN Telecom (Southern Center), Ho Chi Minh City, Vietnam
FPT Telecom, Ho Chi Minh City, Vietnam
FPT Software, Ho Chi Minh City, Vietnam
Guangdong Communications Administration (GCA), Guangzhou, China
Huawei, Shenzhen, China
HPT, Ho Chi Minh City, Vietnam
PCCW, Hong Kong, China
Telestra International, Hong Kong, China
U.S. Consulate, Hong Kong, China
U.S. Consulate, Ho Chi Minh City, Vietnam

Vietnam Data Communication Company, Ho Chi Minh City, Vietnam
VNG (Vinagame), Ho Chi Minh City, Vietnam

The health and global competitiveness of U.S. information and communications technology (ICT) firms are essential to national security and national resource strategy. ICT is a primary force for generating U.S. economic growth and prosperity and therefore a major driver in the global economy. The purpose of this study is to analyze the condition, outlook, and challenges for the primary sectors and markets that make up the ICT industry and use this analysis to recommend government policies that will enhance the ICT industry's contributions to national power. Following the main body of this paper, expanded essays address three pivotal topics affecting the central challenges in the ICT industry today, especially the explosion of data. These three topics are social networking, government implementation of cloud computing, and cybersecurity/ critical infrastructure protection.

The seminar's methodology to gain expertise in U.S. and international ICT industries was to research current events from various media sources, host guest speakers from across the industry, examine specific issues through individual research and topical papers, and visit ICT firms in the United States and abroad. Specifically, the seminar visited firms in Washington, DC, Silicon Valley, CA, Vietnam, and China.

The ICT Industry Defined

The ICT industry uses general-purpose technology that provides "platforms on which many different tools or applications can be constructed"[1] and services that can be delivered efficiently from a great distance over a network. Both of these characteristics are similar to the electricity production model. Consequently, the ICT industry enables the delivery of information across the multiple networks that comprise the national security enterprise, to including the Internet.

This study includes the following eight ICT industry sectors as defined by the North American Industry Classification System (NAICS): 1) Electronic computer manufacturing; computer storage device manufacturing; computer terminal manufacturing; other computer peripheral equipment manufacturing; 2) Telephone apparatus manufacturing; broadcast and wireless communications equipment; other communications equipment manufacturing; 3) software reproducing; magnetic and optical recording media manufacturing; 4) Software publishers; 5) Wired and wireless telecommunications carriers; satellite and other telecommunications; 6) Data processing, hosting, and related services; 7) Other information services, including operating search engines and Internet portals; and 8) Computer systems design and related services. Appendix B provides a detailed description of the sectors, which represent the primary industry segments but exclude some ICT sectors covered by other ICAF industry studies, to include broadcasting and chip production.

Current Condition

The U.S. ICT industry is extremely robust, with significant innovation and sizable available capital for growth, while providing digitally-enabled national security capabilities and improving quality of life for millions of people. ICT is the primary force for generating economic growth and prosperity in the U.S.[2] and is a major driver in the global economy.[3] Inherent gains in efficiency and productivity allowed ICT to account for 25% of U.S. economic growth (GDP per capita) since 1995, despite constituting just 3% of U.S. GDP.[4] ICT importance is such that ICT networks are designated as one of the Department of Homeland Security's eighteen critical infrastructures and key resources (CI/KRs). Recent key trends in the industry include the migration to wireless, expansion of broadband capability, and use of the Internet

Protocol (IP) standard, with a continuing increase in processing capability and convergence of services, especially for wireless devices.

Everything over IP: The flexibility and efficiencies that the use of the IP electronic programming standard provides led most firms in the ICT industry to adopt IP, thus leading to the term "Everything over IP" (EoIP) as most all new software and networks are fully IP capable systems. By moving to IP, data transmissions become more efficient and accessible via broadband connections for services ranging from voice to high-definition video. The convergence of services is forcing consolidation across the ICT industry. For example, wireless and wireline providers are branching into services traditionally provided by segments of the cable and Internet Service Provider (ISP) industry, while some cable and ISP providers are offering Voice over IP (VoIP).

Mobile Revolution: The "mobile revolution" is growing as a result of increased computing capability in ever-smaller devices and components, facilitating broadband Internet access and a variety of software applications via wireless networks. The introduction of Apple's iPhone and iPad concurrently accelerated an explosion of devices incorporating capabilities such as navigation, video, photo, voice, and Internet access. Mobile technology can now network devices in things such as cars, refrigerators, or shipping containers to enable the transfer of data such as geographic position or maintenance requirements. This increasing ability to connect network devices, to rapidly find and share information, and to execute diverse actions from mobile platforms is stimulating massive growth in the ICT industry nationally and globally, enabling increases in productivity and growth for many industries and the effectiveness of many systems, including defense, intelligence, and critical infrastructure systems necessary for national security.

Wireless: Some of the largest growth in the U.S. economy over the last ten years occurred in wireless service providers segment, including firms such as Verizon Wireless and AT&T. Since 2000, the consumer demand for wireless services has grown from 97 million to 293 million subscribers with wireless revenues increasing from $45B to $159B.[5] The increasing quality and extent of wireless networks has also allowed consumers to disconnect their landlines with 27% of U.S. households now using a wireless phone exclusively.[6] The wireless industry provides increasing value to the U.S. economy through efficiencies, and now has a subscriber penetration rate of 91% of the U.S. population.[7] High data rate service demand and industry competition is pushing providers to invest significantly in more efficient, capable systems, such as the rollout of the 3G standard and aggressive initial implementation of 4G/LTE capable networks in a limited number of market areas.

The wireless segment has a high barrier to entry due to the high cost of infrastructure and the limitations of electromagnetic frequency spectrum availability. AT&T, Verizon, Sprint, and T-Mobile, comprises 89% of the market, making wireless a concentrated market, but also providing increased economies of scale and beneficial standardizations. This includes the apparent move to a single LTE standard for the 4G capability, allowing for greater revenues for continuing network modernizations and innovations.[8] With four fairly similar providers and low or decreasing service provider switching costs, customers have significant leverage in the wireless industry segment. Manufacturers or suppliers of the infrastructure equipment however have little leveraging power due to the large number of suppliers internationally and relatively homogeneous products. The result is prices and margins have remained fairly low due to the competitive rivalry between the major carriers. Substitutes are available, such as prepaid wireless phones and wireline service, including Voice over Internet Protocol (VoIP), but their

appeal is limited by the strong preference for mobile devices with service on demand, and the increasing capabilities of those mobile devices.

Cloud Computing: The cost of processing power and storage is continuing to drop and high-speed Internet is becoming more accessible, enabling cloud computing to reduce the cost to firms and individuals. The level of industry concentration for cloud computing providers is low but growing with a few large providers emerging. The industry lacks standards and is highly fragmented, with over 56% of the establishments with fewer than five employees in 2010.[9] Competition is therefore currently nearly pure with low barriers to entry and significant opportunities for larger firms to benefit from economies of scale for enterprise-sized clients.[10] The major essay section of this paper provides additional details about cloud computing.

Social Networking: Internet social networking provided by firms such as Facebook, is experiencing exponential membership growth. Because workers are five times more likely to turn to a person than to a database for information, collaboration enablers such as social networking have proven to be an economic efficiency multiplier.[11] Social networking also leverages online "crowd sourcing" for solutions, which reduces costs, increases productivity, and reduces labor requirements by a factor of a thousand in some cases.[12] The social networking market occupies a 14% market share of a competitive, lightly regulated, low entry barrier, medium high-technology and high growth, $39B internet publishing and broadcasting industry.[13] Six of the top ten Internet sites have integrated social networking, up from zero in 2005.[14] This reflects the consumer and producer benefits being realized by in the commercial sector due to social networking capabilities. U.S. social networking dominates the global market, but there are some international social network strongholds.[15] Facebook is the largest social network site, with more than 600 million users and 123% annual revenue growth between 2006 and 2011.[16] Domestic competitors include MySpace, Twitter, LinkedIn, Salesforce.com, and Classmates.com. China's Baidu and QQ have significant international market share, especially in China where Facebook is blocked, but with relatively smaller 35% and 65% growth rates.[17] The major essay section provides additional details about social networking.

Software Services: The software services sector is experiencing increasing product convergence, creative destruction, firm acquisitions, and targeted offshoring. Although IT consulting is already saturated with firms, it continues to grow as company restructurings for efficiencies are keeping consultants busy integrating accounting, data storage, and other IT systems. The number of IT consulting enterprises grew significantly due to the low cost of entry, despite many acquisitions by the larger players in the market which, in 2010, included International Business Machines Corporation at 6%, Hewlett-Packard Company at 5%, and Accenture Ltd at 5% market share.[18] The software publishing industry contributed the most significant activity in the software services sector, experiencing annual growth of approximately 2% for the last five years. [19] Large software publishers are eagerly purchasing smaller companies owning strategic patents, decreasing the number of firms at an average of 2% annually for the last five years.[20] In 2010, the three largest players were Microsoft Corporation at 25%, Oracle Corporation at 8%, and International Business Machines Corporation at 7% market share.[21] Software publishing maintained relatively low labor expenses and yielded profits through upgrades. These attributes allowed the industry to provide average annual profits of approximately 20% for last five years, with $156 billion in revenue.[22]

Wireline: The wireline segment is highly competitive yet also highly concentrated, with the top four firms accounting for 92% of the cable and ISP market.[23] Customers have economic leverage due to low switching costs and the ubiquitous availability of wireless substitutes, while

infrastructure suppliers have little economic leverage due to the number of low cost suppliers. The high cost of installing a large area infrastructure and many regulations creates a high cost of entry for the wireline industry segment. High-speed bundled services are the focus of many firms, as television, phone and Internet connectivity are being bundled to win customers with ease of use and high-bandwidth connectivity speed.[24] The wireline, cable, and Internet service provider (ISP) segment had $265B[25] in revenues in 2010 and employed almost one million Americans. [26] [27] However, its growth was low compared to the wireless and software service segments. After billions of dollars spent on infrastructure investments in the last decade, notably by Verizon and AT&T for fiber and broadband upgrades for internet service, most of the major providers shifted business models which call for greater investment in wireless infrastructures.[28]

Hardware Manufacturing: The domestic computer hardware manufacturing industry, which includes manufacturers of computers, monitors and peripherals, and telecommunications and networking equipment, is in decline due to the outsourcing of manufacturing to developing countries. The number of domestic manufacturers fell in all three sectors over the course of the past five years due to acquisitions or consolidations, outsourcing, technology improvements and falling prices. The makers of all forms of computers and networking equipment increasingly outsource the manufacture of their products abroad because of the homogeneity of their products and the benefits of low-cost labor. All three sectors experienced lower overall revenue due to increasing imports from primarily Asian sources. Concentration of market share is moderately high in all three sectors; the largest four firms control 62% of the peripherals[29], 65% of the networking equipment[30], and 77% of the computer manufacturing industries.[31]

Research and Development: Although the U.S. accounts for the largest total share of ICT R&D among the Organization for Economic Co-operation and Development (OECD) countries, when evaluating R&D intensity (R&D expenditures as a percent of GDP), the U.S. currently ranks below several OECD countries.[32] Overall ICT innovation in the U.S. has been strong, supported by a highly encouraging culture, which other nations have strived to replicate. Yet the vast majority of industry R&D is focused on development – on the engineering of future products. Few major companies have formal research organizations, and those with the resources available invest relatively little in basic research compared to their expenditure in development activities.[33] Total corporate R&D spending among the Global Innovation 1000 firms was $503B in 2009; declining by 3.5% from $521B in 2008.[34] The drop is the first in more than a decade and attributed to the economic downturn.[35] The top 250 ICT firms spent over $1B for R&D in 2009, with a 4% annual increase since 2000.[36] The Department of Defense R&D investment sustains basic research in high-priority defense areas such as cybersecurity, advanced learning, information access, systems engineering, power distribution, and energy storage[37], but overall federal R&D spending has been relatively flat for nearly a decade.[38]

Challenges

Although the current U.S. ICT industry is relatively healthy nationally and remains a leader on a global scale, it faces significant challenges that threaten its primacy and vitality. This section categorizes those challenges under three principal areas: 1) Challenges in Creating Value and Contributing to Economic Growth, 2) Challenges in Capacity and Commoditization, and 3) Challenges in Cyber Security and Critical Infrastructure Protection.

Challenges in Creating Value and Contributing to Economic Growth

R&D Incentives: The success of the ICT research enterprise reflects a complex partnership among government, industry, and academia. In the face of current fiscal challenges, the near future warrants increased government and industry collaboration to identify and invest in the highest priority R&D initiatives, minimizing threats to national security while maximizing economic competitiveness. For years, Congress temporarily extended the Research and Experimentation Tax Credit rather than pass permanent legislation, due in part to concerns raised by the Government Accountability Office regarding, 1) disparities between taxpayers in the amount and incentive effects of credit received, 2) eligible costs that constitute qualified research expenses, and 3) documenting and substantiating expenses.[39] President Obama's 2012 budget proposes making this tax credit permanent[40] but without resolution to the underlying issues raised by GAO, permanent legislation remains unlikely.

Human Capital and Science, Technology, Engineering and Mathematics (STEM) Education: The U.S. produces a sufficient number of STEM degree holders to meet the demands of the ICT industry. However, too many are choosing non-STEM career paths after graduation, leaving gaps that are filled by highly-skilled immigrant STEM workers. Likely reasons for this exodus include the perception of decreased future opportunities due to job losses in the industry caused by offshoring or the belief that other career tracks may be more lucrative. The challenge is to encourage more students to pursue STEM degrees and to incentivize STEM degree holders to choose careers consistent with their academic credentials. The ability to attract intellectual capital in ICT sectors related to national security is a growing concern.

Export Control: Another major challenge is to reform the outdated U.S. export control system as "[p]oor coordination among the agencies involved in export controls has resulted in jurisdictional disputes and enforcement challenges".[41] This has impeded the success of domestic ICT firms in exporting goods and services abroad and has done little to limit the proliferation of technology related to U.S. national security interests. The Department of State currently makes "commodity jurisdiction" decisions as to whether an item is subject to the U.S. Munitions List and thus subject to Department of State control or, conversely, whether the item at issue is "dual use" and thus subject to Department of Commerce control.[42] However, the Departments of State and Commerce have disagreed, simultaneously claiming jurisdiction over the same items.[43] This poor coordination resulted in numerous lost economic opportunities for ICT firms.

U.S. Competitive Advantage Affected by Emerging Markets: China's competitive advantage in electronics manufacturing is largely responsible for its emergence as India's top trading partner in 2008, supplanting the U.S.[44] This trend is global in scope, and mirrors the evolution of U.S.-Brazil-China trading relationships. Chinese businesses are now encroaching on the economic sectors that spurred and strengthened U.S.-India trade ties. Trends suggest that countries with more evolved ICT industries, such as the U.S., have moved away from lower skilled machine manufacturing and are producing higher value goods and services that focus on developing content in the global information society. The challenge for U.S. ICT industry will be to have the ability to penetrate emerging markets, such as China, to deliver knowledge-based information services which will not only help the industry but will foster greater cooperation and economies of scale within the international community.

Challenges in Capacity and Commoditization

Wireless Spectrum Availability: Barring a breakthrough in wireless technology, nature provides a finite amount of wireless spectrum as defined by the laws of physics. Domestically

the Federal Communications Commission (FCC) is the sole distributor of ten-year wireless spectrum licenses, which form the technological basis for facilities-based wireless service providers. While wireless spectrum capacity is fixed, the convergence of connectivity has accelerated the demand for wireless services, with the average smartphone user already accounting for eleven times more data consumption than a non-smartphone user. Additionally, incumbent licensees, such as the DoD, are very inefficient users of their prime wireless spectrum holdings. Therefore, President Obama directed the FCC to reallocate 500MHz of underutilized spectrum to the wireless industry. However, it will take time to consolidate current users into their new spectrum. The near-term need for spectrum will continue to incentivize consolidation in this market, further frustrating new entrants and growth of current wireless service providers. To meet projected consumer demand, the wireless service providers need continued reallocation of spectrum from inefficient users, enabling the FCC to distribute additional wireless licenses.

Cloud Computing: The Obama administration published a cloud computing strategy and is assisting government agencies to meet designated goals. However, the lack of upfront funding, short planning timelines, and an initial lack of support slowed the process. The next challenge is to develop standards as well as regulations on privacy, security, and ownership of data that will enable the interaction of clouds forming synergies, efficiencies, and collaboration between firms, government agencies, and individuals.

Social Networking: The continued proliferation of social networking has ramifications spanning many future national security challenges.[45] Social networking allows issues and misinformation to go viral rapidly and can define relationships that test national sovereignty against local, regional and other global interests. The challenge is to take advantage of social networking's potential influence to support national security objectives and anticipate emerging issues.[46]

Challenges in Cybersecurity and Critical Infrastructure Protection

Cyber Security: Maintaining cyber security against theft, intrusion, or attack is arguably the greatest challenge facing the globalized interconnected world in the next decade. Targeted attacks from malware have been on the rise. With increasing convergence and connectivity, more people around the world will have access to the Internet to be the sender or victim of cyber-attacks. The challenge is for corporations and the government to develop and enforce policies that will better protect networks from attack. Since President Obama's cyber policy review in May 2009, less progress than expected occurred. The Obama administration is still debating whether it needs new legal authorities to strengthen the government's ability to defend private-sector networks and whether current law even allows such actions.

Critical Infrastructure Protection: Private industry owns over 80% of critical infrastructures and key resources (CIKR). Trapdoors placed by advanced persistent threats are found more frequently in the networks that control Software Control and Data Acquisition (SCADA) systems. The vast majority of CIKR systems are not "air gapped" from the internet and do not have the processing capacity to support encryption. The challenge is to incentivize industry to make the investments necessary to address vulnerabilities and achieve an appropriate level of security.

Outlook

The ICT industry outlook is shaped by market demands for increases in the convergence of capabilities and the need for those capabilities to be mobile and on-demand. This increased

convergence is, in turn, driving increased data requirements, in terms of both storage and distribution. The handling of these fundamental ICT demands will underpin future trends in the economy, in policy and legislation, and in the technological innovation that will significantly shape our future.

Several vulnerabilities could serve as potential impediments to the industry's ability to surge and mobilize in response to a national security requirement. Examples include ICT-related vulnerabilities of the global supply chain and capital-intensive manufacturing of key materials and parts used in the ICT industry (e.g., rare-earths, silicon wafers, and semiconductors). Additionally, weapons of mass "disruption" in the form of cyber-attacks against U.S. information networks could also impede general mobilization, especially when ICT's integral presence in numerous other relevant industrial sectors is considered.[47]

The short-term outlook for the ICT industry is generally positive. Moore's law (the doubling of the number of transistors on an integrated circuit every 2 years) helps drive extremely dynamic technological change in the ICT industry, and explains why many firms in this industry define short term as 18 months or less, as opposed to a five-year outlook used by other industries.[48] In the short term, domestic legislation on issues such as spectrum allocation, net neutrality, privacy, patent reform, and export controls will set the tone for the industry's direction. Government, firms, and individuals will begin to move more of their computing to the cloud as data storage and transmission becomes increasingly commoditized and efficient. International policies related to privacy and data security, innovation and technology transfer, market access, and Internet governance will also affect global opportunities for U.S. ICT firms, frequently in negative ways. For instance, ICT-related manufacturing will continue to move offshore due to higher U.S. labor and capital costs and the highest statutory corporate tax rate in the world.[49] Another driver of this off-shoring trend is the continued move of U.S. ICT manufacturing up the value chain and away from less skilled manufacturing. Nonetheless, the U.S. will lead the world in innovation, particularly further up the value chain in areas such as process engineering and product development.

In the medium term (2-5 years), mobile computing platforms will become the predominant method for web access worldwide. This is already the case in many developing societies lacking wired infrastructure.[50] Ubiquitous access to video, voice and data over IP will become the global norm. Bandwidth requirements will likely grow exponentially, primarily driven by video traffic on demand expectations. The world's submarine fiber backbones currently have enough surplus capacity to handle disruptions such as the Japan earthquake as well as the anticipated data traffic surge.[51] The industry will need to devise innovative technologies to economize and optimize limited electromagnetic spectrum availability, especially as it attempts to deliver data over the "last mile" to mobile clients. Cloud computing will drive growth in wireless and fiber optical networks, particularly as customers demand resiliency, redundancy, and efficiency between multiple clients and data centers.

Machine-to-machine computing will increase as electrical grids, homes, appliances, and global supply chain elements are "made smart" with computer chips and communication technology. Securing and powering massive data centers will emerge as key issues for critical infrastructure protection. U.S. firms are leading much of the innovation and research in this field, but competition is keen from Asia (e.g., Republic of Korea, Singapore) and Europe (e.g., Denmark, Estonia), and even Africa, where mobile telephony is already used extensively for financial services.[52]

In the long-term outlook beyond five years, silicon chip processor speeds and transistor density levels may plateau as physical thresholds are reached. New materials (e.g., carbon or plastic platforms rather than silicon-based) and new methods of computing (e.g. quantum or optical computing rather than transistor-based) will begin to emerge. Additionally, semantic processing will enable machines to independently reason about vast streams of information to rapidly make new conclusions.[53] The growing need for interoperability between applications, databases, and networks will increase reliance on middleware and service oriented architectures while promoting open-source software development. This open-sourcing will reduce development costs but will also expose the U.S. to different risks from foreign expertise in common software languages and architectures.[54]

Global sourcing of intellectual property, labor, parts and raw materials will make it increasingly difficult to determine the national origin of the output of the ICT industry. The rise of the BRIC countries (Brazil, Russia, India, China) will drive global growth, but could lead to the emergence of "walled gardens" in the world where ICT standards differ and either intentionally or unintentionally serve as barriers to entry into these markets. Additionally, the impact social networking will have on globalization, politics, and transparency may encourage some countries to disconnect certain Internet websites from the public. Threats to keeping ICT production within U.S. borders include foreign countries with productive and skilled workers, higher quality manufacturing, and lower labor and capital costs. In countries such as China and India, these trends are the most obvious, and numerous U.S. and multinational firms have already relocated much of their ICT manufacturing, software development, and business process outsourcing to these countries.

While the U.S. still leads in innovation and sophisticated, highly technical production, the future will see both China and India gain ground as their workers become more skilled and their focus on education and innovation pays greater dividends. These rapidly growing countries also present an opportunity for U.S. firms to gain market share in a vastly expanding middle class who will want to take advantage of products like smart phones, personal computing devices, and online services. The sheer size of China and India, with 37% of the world's population, provides market-changing opportunities as their growing middle classes drive demand, both domestically and globally. To put it in perspective, in 2010 China reported having 457 million Internet users, or about 31% of China's population.[55] That number was less than half, or 210 million users, only three years earlier.[56] To be competitive, particularly in Asia, U.S. firms will have to plan strategies that enable them to remain profitable with a growing global customer base that is middle class or poor rather than affluent.

Overall, the global ICT industry's position in the world marketplace will likely increase, with revenues becoming increasingly distributed globally due to the trends mentioned above. This will increase the complexity for policy makers to maintain national competitive advantage, especially as attempts to restrict trade using export controls are likely to make the domestic industry less competitive. For the United States in particular, innovation remains the lifeblood of maintaining a leadership role in this industry, making STEM education and the proactive evolution of technological processes critical, both now and in the future.

Government Goals and Role

The transformative effect of the ICT industry is critical to national security and economic prosperity, both domestically and abroad. A healthy ICT industry is vital to national security as recognized by the Obama administration's May, 2010, *National Security Strategy*. Specifically,

the relationship between technology and national security, and the importance of innovation and investment in research and development. At a minimum, government fosters the environment where markets operate efficiently. However, the government can play a larger role by recognizing weaknesses, anticipating the opportunity to improve performance, and judiciously responding to ICT market challenges by establishing goals and policies that will continue to optimally balance the relationship between security and prosperity. Yet, government must be careful to avoid the risk of excessive intervention. In an effort to stimulate innovation and maintain the narrowing U.S. competitive advantage in the ICT industry, three general categories of recommended government policies follow.

Innovation is Essential for Creating Value and Economic Growth. America should continue to foster the scientific and technological breakthroughs that lead to innovation, fueling our economy and ensuring our national security. Government STEM reforms, such as increasing the number and value of scholarships in return for commitments to enter a STEM field upon college graduation will help produce, attract, and retain the best and the brightest talent necessary to sustain our knowledge-based workforce. The U.S. can achieve further benefits by reforming immigration policies to include a market-based approach for the number of H-1B visas granted, by easing visa requirements for prospective foreign students seeking advanced technical degrees in the U.S., and by offering a direct path to permanent residency for advanced STEM degree graduates. Policies that increase the number of STEM graduates will ultimately provide essential market opportunities to improve the likelihood that beneficiaries remain in the U.S.

In parallel, the government should prioritize budget initiatives and fund those innovations with the greatest potential for transformational applications. Since basic research currently represents only a small fraction of overall ICT industry R&D funding and ICT is the engine that drives economic growth, in our current fiscal situation the government should redistribute funding for research most likely to lead to key development capabilities for the future. Examples that Congress should champion in President Obama's 2012 budget proposal include such high-priority defense areas as cybersecurity, advanced learning, information access, systems engineering, power distribution and energy storage.[57] Multi-agency initiatives focused on processing enormous quantities of data and building foundations for assured computing, secure hardware, software and network design, and engineering to address the goal of making Internet communications more secure and reliable should also be considered for funding.[58]

The government should also facilitate expansion into sizable foreign markets like China, Vietnam, India and even Africa. Numerous economic growth opportunities exist to increase global market demand in ICT. U.S. foreign policy should encourage the Chinese government to achieve openness, transparency and equivalence in mutually beneficial trade, investment and intellectual property policies. Similarly, the U.S. government should encourage the Vietnamese government to enforce piracy laws, improve transparency on the Internet, and improve the regulatory environment for small and medium-sized private businesses to create a better atmosphere for foreign direct investment. Additionally, U.S. foreign policy should assist African governments to develop Internet governance policies aligned with their economic growth strategies to specifically foster the advancement of African intellectual capital. The ICT industry in Africa has vast untapped market growth potential that could be providing improved socio-economic benefits for Africans.

The U.S. government should also continue to advance the President's Export Control Reform Initiative to spur growth of U.S. exports. Efforts should continue to focus on establishing a single export control list, a single licensing agency, a single enforcement-

coordination agency, and a single information technology system to strike the right balance between national security and economic opportunity.

Capacity and Modernization Congress should enact the FCC's National Broadband Plan (NBP) to improve the information system support structure. Among its various options, the NBP specifies affordable and extremely fast Internet access for at least 100 million U.S. homes within five years, apportionment of 500 MHz of additional spectrum for wireless broadband, an overhaul of the Universal Service Fund (USF) to support broadband in rural markets, and service provider access to infrastructure at reasonable costs.[59] Increased broadband access is expected to improve the underlying information system support structure for job growth and education improvement. Admittedly, the relative importance of this factor in relation to others for stimulating economic growth appears to be anecdotal thus far. However, much like the U.S. highway and education systems, internet access is considered a common good.

Inefficiencies in government IT impacts its ability to effectively serve the American people. The U.S. government should resource the Federal Data Center Consolidation Initiative (FDDCI) and "cloud first" policy to reduce hardware and software costs for government data centers while increasing IT security. The government should also execute the Federal Cloud Computing Strategy (FCCS) and the Office of Management and Budget's 25 point implementation plan to set the stage for government-wide business practice transformation that will enable various synergies across government. It should also assist in developing technical and security standards and lead by enacting regulation regarding privacy and data ownership.

The U.S. government should also embrace responsible use of social networking as a key soft power. Because of the Internet, information, regardless of accuracy, now spreads quickly around the globe and has the potential to threaten national security. A national social networking strategy should be developed to be used in conjunction with larger U.S. national security policies. Additionally, social networking capabilities and resources should be integrated across national security funding initiatives to obtain integrated, capability-based benefits.

Cybersecurity and Critical Infrastructure Protection. Cyber threats are a national security concern, but also a threat to national economic interests. Cyber attackers likely have the ability to disrupt America's most vital systems, from electric power grids to financial markets. The government should incentivize activities that promote greater cybersecurity for all users and should regulate standards to protect the most important elements. Guarding against cyber-attacks and protecting America's critical infrastructures warrants greater government action to require risk assessments, compliance with common information security policies, planning at the appropriate level of transparency, and baseline security training and certification. The government should also build a new online "identity ecosystem" in which transactions for both the public and private sectors are more secure and therefore more trusted.

Essays on Major Issues

Social Networking. Social networks are the "pattern, or structure, of relations among a set of actors".[60] Online, social networking is an exponentially growing, synergistic component of the ICT industry that will continue to affect the global community in business, government and personal arenas. The power of social networking is evident by its epidemic-like spread, deep societal penetration, and demonstrated ability to transform diverse world events. Government

should not ignore social networking due to associated lower service costs, increased government service capability, accessibility, and other opportunities that could increase demand and services outlay, especially with respect to national security.

Social networks historically provided benefits of greater interaction, and today they are distinctly more evolved, accessible, far-reaching, and easier to use than ever before. Early Internet technologies evolved to facilitate greater social expression in current Web 2.0 applications, allowing users to interact and collaborate with each other in a social media community dialogue as creators (prosumers) of user-generated content.[61] The social networking market occupies a 14% market share of the competitive, high growth $39B Internet publishing and broadcasting industry.[62] The industry structure is currently characterized as having unclear operational boundaries, high user demand, light regulation, and low barriers to entry. Social networking boasts six of the top ten Internet sites where before 2005 there were none.[63] Social networking is now being optimized for the growing mobile Internet community, and contains a diverse set of companies. The largest social network site, Facebook, has more than 600 million users and has demonstrated 123% annual revenue growth between 2006-2011.[64] Twitter has been adding approximately five million new users per week[65], followed by niche competitors LinkedIn, Salesforce.com and Classmates.com.

Social networking business models vary primarily by subscriber usage, visitor access rate, and advertiser service choice. Revenues are derived from on-line advertising and premium service fees above free baseline services. The industry remains competitive, innovative, and consumer-driven despite Facebook's significant lead over competitors. Additionally, users have low switching and minimal (if any) actual participation costs, making cost leadership strategies untenable. The current industry environment is relevant, healthy, and growing in both global and niche markets. The U.S. social networking services base dominates the global market, but there are some international-based regional social network base strongholds.[66] Facebook and Twitter are market leaders with 110% and 1,107% annual growth in 2010, respectively. [67] Foreign companies like Baidu and QQ have seized respectable regional market shares, but with comparably small 35% and 65% growth rates. [68] The novelty of social networking means many dynamics are unpredictable and it conceivable that a new social networking firm could become a moderate market leader in the future.

Social networking's relevance, power, and demand are a result of the unprecedented levels of innovation, collaboration, and productivity that have resulted from this new medium of information exchange. Social networking aggregates attributes, extends skill sets, and provides the informational catalyst that accelerates the productivity of governments, businesses, and individuals. Empowering commerce, technology, media, and culture to spill across previously-closed borders, these capabilities readily provide people with knowledge and solutions in this 24/7 world that craves affordable, efficient coordination. [69]

Innovation created by information exchange through social networks is becoming more and more essential to compete in today's volatile environment. New ideas are key elements to improve the effectiveness of integration, socialization, development, and delivery.[70] Innovation growth in the enterprise environment is a result of finding expertise and facilitating open participation to integrate efforts,[71] tap new expertise, identify unarticulated needs, and gather new inputs to solve complex issues with an expanded resource set and deliberate solution base.[72] A focused study of 60 organizations showed that well-managed network connectivity is critical to innovation.[73] It suggested that intimacy permits innovation and synergy especially in dynamic environments, such as during new product development or continuous improvement processes.

Social networking's key agent for change is collaboration. Flat organizations and a more globalized world require different perspectives, wider resources, and an integrated effort to achieve strategic objectives. Today, we continually witness examples of Goliath-sized problems that single players cannot tackle alone, and organizations are increasingly networking outside themselves to leverage multi-lateral partners. In today's resource-constrained environment, objectives prove to be more achievable when diverse teams work together.

Arguably the most important social networking capability that affects the bottom-line is productivity. If social networking did not bring a benefit that exceeded costs, it would quickly be discarded. In today's case, social networking is an undeniable accelerator that leverages humans by "crowd sourcing" which can significantly reduce costs, increase productivity, and reduce manpower requirements by a factor of a thousand.[74] Although some studies have determined that increased social networking among students has yielded less study time and poorer grades,[75] two other studies suggest a 9% productivity increase[76] and a 46% innovation increase.[77] Over 60% of the top 100 online retailers now reach customers via social networks.[78] The top 25 businesses that use social networking have been able to increase their aggregate target audience by 318 million people. The top 50 businesses have increased it by nearly 450 million people.[79] In 2007, social networking eclipsed email as a communication vehicle,[80] lending proof that users are valuing its "network effects".[81]

By traditional business methods, value for social networking remains largely unmonetized, with values more typically defined in less tangible individual-utility terms. The lack of specific value definitions by industry leaders suggests there is a dominant perceived value in using social networks. Social networking's benefits include shared resources, capabilities, and progress towards common interests while achieving reduced costs, improved efficiency, and better effectiveness. The information exchange, collaboration, and innovation that encourage increased productivity have become a key to competitive advantage. At the most basic level, social networking is valued because it humanizes technology's capability to improve mass communication.[82] Social networks can also support analytical tools that add to "social business intelligence". As attempts to monetize social networks continue, the prevalent "ubiquity first, revenue later" business strategy[83] has been successful to date. Ultimately, monetization will probably rely on multiple aspects beyond advertising and subscription to include virtual goods, branded content, allied services, location search, and location-based information.[84]

Virtual social relationships can be legitimate and powerful, and most worthy of pursuit in a targeted manner. Social networking increases "social capital", strengthens strong ties, and maintains less productive ones.[85] The events in both the Philippines and Egypt reveal the effects of strategic coordination now possible with social networking.[86] Both the anti-Estrada Philippines and anti-Mubarak Egypt movements showed how larger, looser groups can organize and create a "dictator's dilemma".[87] Some even suggest that without social networks, President Obama would be neither elected nor even nominated.[88] Although social networks can achieve significant results across the spectrum rivaled by few other mediums, its' effects can be stifled by closed political systems. These government environments can force social network providers to play by government imposed rule sets or be subjected to enormous restrictions or complete shutdown. Such intervention eliminates the social network value and decapitates its capabilities resulting in little or no use as well as inconsequential consumer benefits. The impact of a closed political system's influence on a social network can greatly reduce or eliminate productivity, collaboration, and innovation as it looks to protect its power and sovereignty.

Social networking is destined for further change and market evolution. The dramatic growth of global technological connectedness promises increased development. First, social networks will become increasingly mobile and more valuable. Mobile will become much bigger than desktop utilization by 2014 and grow at faster rate than desktop Internet.[89] With the emphasis and growing demand, game-changing communication and commerce platforms will emerge to more effectively serve the greater consumer demand base. Data will become of primary importance, with video trailing.

Second, social networking services will trend towards targetable environments and become more pervasive.[90] It is reasonable to expect that services will find a niche in a majority of areas affecting everyday life. For instance, Facebook already started offering movies. Third, expect innovators who grow new capabilities that challenge existing networks and services to challenge today's market leaders. A current subscription base is no guarantee of future advantage. Services need to remain highly competitive through innovation due to the high threat of substitution. It is reasonable to expect services to target the true value-added networks or niches that focus on family, business, professional interests, dating, and friends.[91]

Fourth, commerce, and especially e-commerce, will benefit and grow larger as a result of social networking largely driven by mobile capacity and social networking's increased influence. Fifth, security, privacy, and vulnerability concerns will continue to threaten social networking services.[92] Ultimately, if social networks provide safeguards that ensure user confidence, the increasing cyber security challenge will be mitigated. A demonstrated inability to achieve that confidence may undermine networking's long term sustainability.

Sixth, the vision for social networking will be evolutionary and unpredictable. Technology will naturally proceed to areas of increasing value, efficiency, and quality of service. Perhaps contradictory to today's sentiment, social chaos or reduced societal control may bring immense opportunities for greater use of social networking.[93]

Despite its rapid growth, quick adoption and associated benefits, social networking is still embryonic in many ways. From a national security perspective, social networking proliferation has ramifications spanning many future challenges.[94] Governments may harness social networking's influence to support national security objectives and anticipate emerging issues.[95] Social networks are a key soft power component the United States should embrace to pursue its interests and promote global stability. Finally, networking can cause issues and misinformation to go viral and global fast, testing national sovereignty against local, regional, and global parties.

Four key recommendations are:

(1) Incorporate social networking into the National Security Strategy as a balanced, force-multiplier contributor to national strategy and resource objectives.

(2) Appropriately network our national competencies, resources, and actors to bring to bear our full capabilities and capacities.

(3) Address threats and actors that intentionally attempt to destabilize value-added social networking objectives.

(4) Integrate social networking capabilities across appropriate national security initiatives to obtain capability-based benefits.

- Captain Ron Florence, U.S. Navy

Government Cloud Implementation. The Obama administration perceived a need to make significant changes in the way the government implements and utilizes IT. The February 2011

Federal Cloud Computing Strategy (FCCS) characterizes the current federal IT environment by "low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times" which negatively impacts the ability to serve the American people.[96] To address this, the administration has implemented a series of policies to fundamentally change the way the government provides IT services while significantly reducing the federal IT budget. This essay addresses the changes that are occurring as a result of the administration's initiatives, including the FCCS, OMB's February 2010 Federal Data Center Consolidation Initiative (FDCCI), and the December, 2010, 25 Point Implementation Plan (25PIP) to reform federal information technology management. This essay also addresses challenges agencies are encountering while trying to implement the directives and makes recommendations for government policy changes to create synergies. Agency roles, responsibilities, and implementation plans to meet the Obama administration's directives are provided in Appendix C.

In February, 2010, federal Chief Information Officer (CIO), Vivek Kundra, implemented the FDCCI, the first of the administration's key IT initiatives. The goals were to reduce the overall energy requirement, real estate footprint, amount of hardware and software, and operating costs of government data centers while increasing the overall IT security posture.[97] Federal data centers grew from 432 in 1998 to 1,100 by 2009. Kundra determined that much of the infrastructure was redundant, inefficiently used, and unsustainable, and that maintaining each data center was a significant cost.[98] Skilled personnel required to run the data centers is an additional cost. This initiative established a series of deadlines requiring federal agencies to inventory all assets and develop data center consolidation plans by August, 2010, which required OMB approval by December 31, 2010.[99] This set the stage for subsequent consolidation plans and the movement to cloud computing.

The intent of OMB's 25PIP was to clear the obstacles that kept the government from implementing best practices and "allow agencies to leverage information technology to create a more efficient and effective government."[100] A key directive was the "cloud first" policy, requiring each agency to move three services to the cloud within 18 months, the first one within 12 months, and to reduce the number of data centers by at least 800 by 2015.[101] The 25PIP also addressed problems with IT program management.

The FCCS provided tools such as templates, information, security guidance, and contracts that federal agencies can use to more rapidly move to the cloud. This strategy targets $20 billion for migration to cloud solutions out of the government's $80 billion IT budget.[102] The Obama administration believes cloud computing will provide reliable and innovative resources in a constrained environment, enabling agencies to save money by paying for only the IT resources they use. The cloud will also allow agencies to utilize economies of scale to rapidly expand, contract, or surge capacity, share infrastructure, and become more efficient, agile, and innovative. In addition to laying out the proposed benefits of cloud computing, the FCCS provides a framework for decision-making to support agency migration, highlights implementation resources, and identifies Federal roles and responsibilities for cloud computing implementation.[103] It outlines methods to improve server utilization from the current 30% average to 60-70% utilization.[104]

The tools provided by the FCCS were designed to accelerate data center consolidation and cloud implementation by assisting agencies in the planning, purchasing, and implementation of their efforts to meet the FDCCI. Practical guidance was provided for the selection, planning, security, and procurement of government cloud solutions at all levels. These tools would have

been more helpful if they had been provided before the 25PIP required agencies to begin executing under a short timeline with insufficient guidance, information, or assistance. Unfortunately, the FCCS was released late in the implementation process, exacerbating some of the challenges agencies have encountered. Because data center migration is a complex and expensive task, the greatest challenge to implementing guidance has been a lack of upfront funding.[105] This was also the bane of a 1995 data center consolidation plan.

Data security and storage policies are another challenge. The government is expecting significant security benefits from cloud computing, to include the ability to focus resources at fewer sites that touch the Internet. However, federal agencies are concerned about where the data is stored, who has access to it, and if it shares storage with other organizations' data which could possibility lead to data spillage. Transparency is a major factor influencing agency decisions to outsource as agencies want to understand how the policies, people, and technologies are managed to secure the data center.[106] For some agencies, this could pose a national security concern if a provider's virtualization takes data outside of the U.S.

Cloud computing could pose new security risks as sensitive data is migrated to locations not directly under government control and could reduce options during a cyber attack by providing fewer data locations and less flexibility in response. Changes to internal culture are causing some anxiety due to the lack of physical data control in the cloud implementation. Political challenges also exist due to federal jobs lost in states where data centers are closing.

Many agencies have already plucked low-hanging fruit by moving services to the cloud such as email, web services, and collaboration software while they determine how to handle the more difficult applications. Several bigger agencies are making progress with data center consolidation but smaller agencies are typically making server room consolidations instead and adopting virtualization and cloud computing services. Most larger agencies seem to be implementing private clouds or are using mixed solutions, but many smaller agencies have turned to public providers.

Some state governments have also begun data center consolidations and are offering services to their counties and municipalities. At the municipal level, several of the larger cities have outsourced to public clouds. Counties and small municipalities have been mixed but many are looking to utilize state or federal cloud resources.

The initiatives have thus far not met the desired savings goals. In September, 2010, an independent assessment of the FDCCI stated, "while some agencies have made progress in consolidation, lack of funding, inadequate planning time, and insufficient resources present major obstacles to the initiative being the game-changing program that it could be. However, over the long-term re-architecting federal data centers will put the federal government on a faster trajectory to adopt cloud computing than would have otherwise been possible".[107] Agencies must overcome the challenges of an abbreviated planning and implementation timeline, lack of upfront funding, technical obstacles, and cultural and political roadblocks.[108]

Industry-wide, there are several obstacles to widespread adoption of the cloud. These are concerns about data security, privacy, and ownership, the absence of global industry-wide standards, and protection of the interests of competing cloud users.[109] Since standards are not finalized, unwary subscribers risk getting locked into proprietary systems that will preclude the benefits of cloud utilization beyond their own agency or cloud. IBM expects the development of common security and data standards and assessment tools within the next four years.[110]

Quality of Service (QOS) is another area of concern. According to a 2010 Symantec Disaster Recovery Study, most cloud providers are unprepared and under-resourced to ensure

service through down time, with sufficient backup and recovery capabilities. Typical results from the survey are that providers have an average of four downtime incidents per year lasting an average of five hours.[111] According to the same survey, 44% of data on virtual machines is not properly backed up to include mission critical applications and data and 60% of virtualized servers are not covered in current disaster recovery plans.[112] Agencies migrating to a cloud solution could be at risk of being cut off from and even losing their data. Significant downtime or loss of data can significantly affect user confidence and agency capability. Service level agreements should address privacy, ownership, data access, data spillage, and security, and a thorough risk assessment should be conducted before deciding upon a cloud strategy.

The U.S. government can stimulate industry by implementing statements of agreement between applications, by using better encryption and credentialing, and by incentivizing activities that promote greater cyber security and training. Research is advancing in this area with organizations such as the Open Cirrus test bed and the Open Cloud Consortium (OCC). The latter example is formed by several universities and IT companies to develop standards for cloud computing, establish benchmarks, advance open source reference implementations, manage an open cloud test bed, and sponsor workshops.[113]

True government synergy requires using cloud computing in a whole of government sense. Standard business practices should be developed to enable agencies to outsource transactional processes and focus on the ones where they provide value. The cloud should provide a platform for collaborating with other organizations and facilitate the development of totally new and better business models.[114] Cloud computing allows the combination of data from multiple sources and common formats that make for more effective data sharing and collaboration.[115] These models will grow exponentially in value when interconnecting processes across all levels of government, allowing agencies to work together instead of alone. Process variations between interacting organizations cause complexity, generate large training costs, and make compliance difficult to manage.[116] The synergy of transforming business practices onto the cloud will provide benefits far beyond the dollar savings currently being directed, and will facilitate greater streamlining of processes.

In conclusion, the Obama administration's cloud strategies have advanced considerably, with goals, resources, information, and tools designated to empower agencies to actually implement directives. In the long term, these strategies will save money and improve performance but the lack of upfront funding, short planning timelines, and an initial lack of support made it difficult to get started. Although the administration has still not fully addressed funding issues; the publishing of the Federal Cloud Computing Strategy provided tools to fix many of the initial shortfalls. The next cloud strategy should direct the transforming of businesses processes and the development of synergies across all agencies and levels of government to enable greater effectiveness, collaboration, participation, transparency, and responsiveness between agencies, firms, and citizens.

- Colonel John McLaughlin, U.S. Army

Cyber Security and Critical Infrastructure Protection. President Obama's announcement of a cybersecurity push in May, 2009, and the accompanying cybersecurity report (known as the Hathaway report), contained ideas long called for by various cybersecurity experts. The president also announced that the U.S. government will create a national cybersecurity education program and invest in cybersecurity research and development. However, the effort shows little

progress and lacks details on how to counter the emerging threat. The "cyber czar", Howard Schmidt, announced the Comprehensive National Cybersecurity Initiative (CNCI)[117], in April, 2010, a ten-point action plan identical to the 2009 Hathaway-report.[118] Considering that 90% of the U.S. government's data traffic travels over non-government networks, there is a legitimate concern that the government protect the Internet against theft, espionage, and cyber attacks.[119] Identification of the cyber threats and recommended actions to promote cyber security are provided below.

As malware numbers continue to climb, traditional forms of security such as signature-based antivirus software has become less effective. In 2009, estimates indicated the overall cost of cybercrime to be as much as $1 trillion on a global basis.[120] Cyber criminals now have automated tools capable of releasing very large volumes of malware with extreme variety and sophisticated features.[121] According to McAfee, the first six months of 2010 was the most active half-year ever for total malware production.[122] Symantec also reported the government/ public sector had become the most targeted industry for malware with 1 in 75 emails (1.3%) being blocked as malicious. Large-scale botnet insertions are now being used more frequently to hide more targeted malware in large numbers of "zombie" machines. This makes targeted attacks much more difficult to trace or attribute.

The move to cloud computing will continue as organizations strive to save money and add flexibility to their operations. The cloud may become an enabler for delivering more scalable, comprehensive, and affordable security. Through the cloud, computers will be able to pass threat information back and forth, so that if one organization uncovers a specific attack, data can be shared quickly and easily among a wide network of security professionals.

The sheer volume of cell phone users around the world highlights a need for proactive mobile security measures. While more than 1.5 billion people use the Internet daily, over 4.5 billion use a cell phone every day, creating an attractive target for cyber criminals. As phones become less expensive and more powerful, this number is expected to double or even triple, enabling people in even rural areas of the world to easily access the Internet. Smartphones are the new computers. An estimated 2 billion of them will be deployed globally by 2013.[123] This may yield hidden dangers, because many people tend to think of their phones as innocuous, protected devices. Smartphone types initially varied so much that it was difficult for cyber criminals to take advantage of them, but as the majority of phones are now being built on a few core operating systems, including Windows, Android and Mac, the smartphone world is becoming less secure. Phones have further constraints such as battery life that make traditional security measures, which require the continuous running of software in the background, unrealistic. Attackers can now easily gain access to personal data by taking advantage of the many vulnerabilities of smartphones users, including email, Internet applications, and text messaging. Less than 1% of all smartphones currently have any form of security.[124]

In addition to malware's privacy concerns, another rising concern is the possible destruction and malfunction of physical systems in critical infrastructures. While there are differing opinions, in terms of how real this threat to physical systems is, according to one source,[125] "It is known that there are vulnerabilities that would allow cyber criminals to reach into physical systems, and we are aware of the sophistication of today's attackers. So to think that physical systems are not at risk is really having your head in the sand." Nation-states not friendly to the U.S. are believed to be testing systems to facilitate the takedown of critical infrastructure including power grids, communications systems, emergency services, and financial systems. The compromise and takedown of these systems would cause confusion, chaos, and

hysteria, damaging domestic affairs within the U.S. As physical systems become more connected to the Internet, the kind of attacks we have seen in other areas could show up here as well, a concern that requires the collaboration of various experts to fully understand and prevent.

One consideration for increasing individual system security is to create more secure operating environments. This can be accomplished by writing more secure code that minimizes vulnerabilities and by using decentralized operating systems on cloud interfaces. For example, operating systems like the Google Chromium system minimize the amount of data on the interface, making the user interface more secure by accessing applications and data files through a secure thin client (such as Google's solid state CR48 laptop). The architecture helps protect the confidentiality and integrity of the user's file system even if an attacker exploits an un-patched vulnerability in the rendering engine. Treating the rendering engine as a black box reduces the complexity of the browser kernel's security monitor and avoids constant security prompts. [126] Each interface user has a more isolated operating environment, using a modular browser architecture, keeping only necessary data in the system cache and deleting any unnecessary files after logoff or shutdown. Vital information is retained in a centrally-secured cloud.

The draft National Strategy for Trusted Identities in Cyberspace released by the Obama administration on June 25, 2010, would theoretically simplify handling sensitive documents electronically in a secure Web environment by creating a new "identity ecosystem" that doesn't require user names or passwords. This cyber-ecosystem plan would base authentication on trusted digital identities, laying a blueprint for an online environment in which public and private transactions are more trusted. This strategy identifies the federal government as "primary enabler, first adopter and key supporter". Furthermore, the language of the strategy states, "In the envisioned identity ecosystem individuals, organizations, services, and devices would be able to trust each other because authoritative sources establish and authenticate their digital identities." Trusted providers such as banks would issue security credentials that would then be accepted by other online resources such as social networking sites and e-mail providers. Users would have the credential on a device that would authenticate his or her identity to the computer and, by extension, to services that accept the credential. The strategy includes references to smart cards, USB drives, mobile devices, software certificates, and trusted computing modules as possible authentication technologies.[127]

The next challenge is getting corporations who operate on the Internet to share information that can generate ideas for how to defend against threats. Indications are that only 42% of infrastructure corporations participate in government partnership initiatives like IT-ISAC, and the participation appears to be mainly data collection by the government.[128] Security concerns include unintentionally providing classified data to corporations and the risk of data leakage to cyber criminals and terrorists. Even in cases where a member of a corporation is given clearance to see data indicating a threat, that person may be a supervisor or executive that does not have the ability to take actions to correct the problem and, due to security concerns, can't give the data to the people within their organization that can take the appropriate action.

Improving the security of Critical Infrastructures and Key Resources (CIKRs) will require the appropriate testing of CIKR systems and dissemination of relevant metrics to facilitate the appropriate security activities. In the current economic environment, corporations appear less likely to absorb costs for increased security and, if there is no apparent loss of service, customers do not appear willing to pay for it. Two thirds of infrastructure executives surveyed indicated cuts had been made in cybersecurity due to the current recession.[129]

Additionally, Appendix A of the 2009 National Infrastructure Protection Plan repeatedly mentions encouraging national, state and local agencies and infrastructure owners and operators to take actions to manage their security and share information about cyber threats within their industry, but provides no indication of how.

Many industries would prefer to be left alone and let the market decide how much security is necessary, but that is inadvisable. The private industry will not take into effect the negative externalities caused by failures to secure infrastructure sufficiently, leaving the government to absorb these costs. Therefore it is necessary to provide legislation keyed to performance metrics rather than compliance metrics. Compliance necessitates certain measures are put in place, which places the burden of devising the measures on the government's understanding of each infrastructure's IT systems, not on whether the organization, which understands its systems best, can put the appropriate measures in place to defend against attack.

The next step to create beneficial behaviors in infrastructure industries is to provide metrics-based incentives. These standards could also be scaled over an appropriate timeline to increase protection levels. Built-in physical resilience may counter cyber vulnerabilities from successful attacks. Costs may indicate it is too difficult to create networks that can achieve the required rates of security. Therefore, an infrastructure company can build resiliency within their systems by providing redundancies that can compensate for other system failures so, for example, the loss of one power supply system can be absorbed by other power plants until recovery of the primary. Another method is to provide sufficient physical fail-safes (for virtual control of valves, switches, etc.), that can counter cyber failures and prevent cascading damages. The appropriate legislation should incentivize industries to protect against physical risks while also defending against cyber threats.

The next question requiring legislative action is: What measures are private corporations allowed to use for defense? There are laws within the United States that prohibit hacking activities, but they only affect those hackers within our physical borders. The Internet is a global commons that provides anyone, anywhere, with a conduit to access any system that is connected. If critical infrastructure is being attacked from servers hosted in other countries, does that company or entity have the right to counter attack to prevent further damage? Is it required to that a government entity be informed? There is no specific international agreement that governs cybersecurity or active defense. It is necessary through the World Trade Organization, the United Nations, or another appropriate international body to broker appropriate treaties that codify responses to cyber-attacks. This will protect private corporations from legal response to defensive cyber activities.

- Colonel Trond Lundberg, Norwegian Army, and Commander George Segredo, U.S. Navy

Conclusion

Despite its modest share of U.S. GDP, the ICT industry is a major enabler of economic growth. Information and communication technologies have become extremely pervasive, especially with the impressive growth of wireless communications to the detriment of wireline communications. This trend will continue thanks to the on-going convergence toward mobile devices, communication standards, and online services, connecting more users around the world, and enabling new economic and social models.

Yet, the ICT sector faces challenges and externalities that may require government involvement. First, the government can help sustain value creation by incentivizing long-term

research, providing the industry with the right number and level of STEM-qualified workers, and building the appropriate international trade environment to sustain a high level of international competitiveness.

Second, the ICT industry faces challenges in capacity and commoditization, such as wireless spectrum availability, cloud computing and social networking. The government has to prove its ability to manage wisely the delicate issue of spectrum allocation and take advantage of all the efficiencies provided by new technologies, while avoiding their traps.

Finally, cybersecurity and critical infrastructure protection are major concerns for the government to sustain the pace of growth of the ICT sector. A major cyber-related disruption may negatively affect the material lives of citizens and their confidence in government to protect them. Though most firms indicated the high importance of cybersecurity and customer trust in their ability to protect against cyber threats, indications are that actions by firms to this point are insufficient and, as long as the immediate impact is insignificant, consumers' desire to pay for cybersecurity is minimal. Therefore, there is a significant need for government involvement, including possible legislation and international agreements. The government may also conduct monitoring and analysis, to incentivize firms to enact better security protocols throughout critical infrastructures and business systems that affect national security.

Influencing a successful market is a delicate issue. However, balanced governmental involvement appears necessary to guarantee the future competitiveness of the U.S. ICT industry, and to address concerns linked to national security.

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)
Dan Gordon, Valhalla Partners
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)
Elaine Wu, USPTO
Jim Young, Google

Appendix B - The ICT Industry Defined

For this study, the ICT industry includes: **1**) computer manufacturing (the manufacture, design or assembly of personal computers, laptops, handheld computers and servers); **2**) telecommunication network equipment manufacturing (the manufacture of wired [voice and data] telecommunications equipment, including telephone switching systems, telephones and answering machines, data bridges, routers, modems and gateways); **3**) magnetic and optical recording media manufacturing and software reproducing (manufacturing optical and magnetic media, such as blank audio tapes, blank video tapes, and blank diskettes and/or mass duplicating audio, video, software, and other data on magnetic, optical, and similar media as well as mass reproducing computer software data and programs on magnetic or optical media, such as CD-ROMs, diskettes, tapes, cartridges or game cartridges); **4**) software publishers (producing and distributing computer software, such as designing, providing documentation, assisting in installation, and providing support services to software purchasers); **5**) wired, wireless, satellite and other telecommunications (providers of direct communication services, such as local, long distance and international phone service using wired telecommunications networks; operate and maintain switching and transmission facilities to provide direct communications via airwaves and provide services to include cellular mobile phone services, paging services,

broadband personal communication services and wireless public safety services; engage as third-party distribution systems for broadcast programming and deliver visual, aural, or textual programming received from cable networks, local television stations, or radio networks to consumers via cable or direct-to-home satellite systems on a subscription or fee basis; and provide Voice over Internet Protocol services to consumers, businesses and government organizations); **6**) data processing, hosting and related services (providing infrastructure for hosting or data processing services to include providing specialized hosting activities, such as web hosting, streaming services or application hosting; providing application service provisioning; or providing general time-share mainframe facilities to clients); **7**) other information services (providing Internet access through wired infrastructure [including copper wire, coaxial cable and fiber optics] as well as renting or leasing out capacity on networks to support the network infrastructure of other companies [backhaul]; and operating search engines, Internet portals and other types of websites that display advertisements; **8**) computer systems design and related services (providing expertise in the field of information technologies through one or more of the following activities: [a] writing, modifying, testing, and supporting software to meet the needs of a particular customer; [b] planning and designing computer systems that integrate computer hardware, software, and communication technologies; [c] on-site management and operation of clients' computer systems and/or data processing facilities; and [d] other professional and technical computer-related advice and services).[130] These sectors are represented by the following 8 codes as defined by the North American Industry Classification System (NAICS):

NAICS Code	Description
3341XX	Electronic computer manufacturing; Computer storage device manufacturing; Computer terminal manufacturing; Other computer peripheral equipment manufacturing
3342XX	Telephone apparatus manufacturing; Broadcast and wireless communications equipment; Other communications equipment manufacturing
3346XX	Software reproducing; Magnetic and optical recording media manufacturing
5112	Software publishers
517X	Wired and wireless telecommunications carriers; Satellite and other telecommunications
5182	Data processing, hosting, and related services
5191	Other information services
5415	Computer systems design and related services

Appendix C – Cloud Computing Defined, Agency Roles and Responsibilities under FCCS, and Status of Migration

WHAT IS CLOUD COMPUTING?

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned or released with minimal management effort or service provider interaction."[131] There are three categories of service: Software as a Service (SaaS) allows users to

access software online as needed and is focused on end-user requirements by supplying the complete and maintained software, which is customizable within limits.[132] It provides applications to the users on demand. Platform as a Service (PaaS) provides the hardware, software, applications, and life cycle of services and hardware. Finally, Infrastructure as a Service (IaaS) makes remote hardware available for data processing in a virtualized environment. Through virtualization, the interface on the guest's hardware acts like a real computer but the software is resident on a remote host.[133] It provides a fully outsourced computing environment, precluding the purchase of servers, software, networking equipment, data-center space and power, and employees to maintain it.

The FCCS discusses cloud models that agencies can choose from to meet their implementation. These are private cloud which is managed within an organization either in house or by a third party; community cloud in which the infrastructure is shared by several organizations; public cloud which is hosted by public companies and is open to the general public or industry; and hybrid cloud which is a combination of two or more clouds that can conduct load-balancing between them.[134]

FDCCI, FCCS, AND 25 PIP DELINEATED ROLES AND RESPONSIBILITIES

The FDCCI designated Richard Spire, CIO for the Department of Homeland Security and Michael Duffy, CIO for the Treasury Department to lead the effort within the Federal CIO Council.[135] The FCCS delineated responsibilities across government. NIST is responsible for coordination across all levels of government, the private sector, and the international community to identify and prioritize cloud computing standards and guidance. GSA is responsible to develop government-wide procurement vehicles and government-wide cloud based applications. DHS will monitor security issues and set standards. Agencies are responsible for determining and sourcing their cloud strategies. The Federal CIO Council is responsible to drive government wide cloud adoption, identify new technologies, and share best practices and templates. Finally, OMB is responsible to coordinate across government and set overall cloud related priorities and provide guidance to agencies.[136] This approach should prove to be effective for synchronizing roles and missions across the government. It is facilitating reaching the Administration's goals to make government more responsive, operationally effective, cost efficient, transparent, participatory, collaborative, and innovative for the citizens it serves.[137]

One of the valuable aspects of the FCCS is that it provides a framework for agencies to use in trying to determine which cloud employment is best for them. OMB, GSA, NIST, and DHS have all developed practical guidance on issues related to security and procurement. NIST and GSA frequently run government cloud computing working groups on topics such as standards, reference architecture, taxonomy, security, privacy and business use cases. This is very useful for agencies implementing their portion of the 25 PIP. Through GSA, the FCCS provides government-wide Certification and Accreditation (C&A) to help agencies migrate.[138] GSA has implemented a contract that currently pre-approves 12 cloud vendors enabling any agency to pick a government approved, certified, and accredited vendor and use this contracting vehicle to procure the cloud capability they need.[139] Agencies can now purchase business applications, productivity tools, collaboration, social media applications and infrastructure as a service such as storage, virtual machines, and Web hosting via the GSA cloud storefront Apps.gov.[140] It also enables them to compare side by side what the different cloud providers are offering. GSA is working on awarding a government wide contract for software as a service and email solutions. Their email as a service expects to save 44% over existing on premise email solutions.[141] Although they have not established a contract with platform as a service, GSA is looking to add

this capability. It is also implementing riders that will allow state and local governments to take advantage of the Federal Government contracts.

Due to the FCCS, DHS and NIST have been instrumental in providing guidance and working groups in order to strike a balance between security and risk. According to the FCCS, much of this has been addressed as part of the 2010 Federal Risk and Authorization Management Program (FedRAMP). "FedRAMP defined requirements for cloud computing security controls, including vulnerability scanning, and incident monitoring, logging and reporting."[142] The government is expecting significant security benefits from cloud computing to include the ability to focus resources at fewer sites that touch the Internet. Fewer sites will enable greater resourcing for stronger platforms with greater reliability, maintainability, improved backup and recovery capability.[143] The current system of Assessing and Authorizing (A&A) is expensive, time consuming and inconsistent across government requiring up to six months and 180K per event. Under the FedRAMP "approve once, and use often" an agency can accept security authorizations performed by other agencies with confidence in its standardization and consistency. This should reduce cost, expedite acquisition, and improve integration across various clouds supporting government.[144]

According to Vivek Kundra, challenges with program management remain pervasive across Federal Government due to a general shortage of qualified personnel. "we continue to see projects spiral out of control – wasting tax payer dollars, failing to deliver results, and introducing security vulnerabilities."[145] The 25 PIP attempts to address this shortfall and inefficiencies by termination of one third of underperforming IT projects, dedicating program managers, staff, and IT acquisition professionals to IT programs, and a modular approach providing functionality every six months.[146] The Office of Personnel Management (OPM) created a career path to attract and reward top performers and is drafting a competency model to cultivate the highest performing managers in IT. This will help generate best practices, innovations in IT management, and greater efficiencies and effectiveness.[147]

The tools the FCCS provided greatly expedite implementation time and effort. These tools would have been extremely helpful before the 25PIP required agencies to begin executing under a short timeline with insufficient guidance, information, or assistance. Unfortunately, the FCCS was released late in the implementation process. The 25 PIP put agencies under a short timeline to implement changes. The agencies lost several months on their short deadlines struggling until the FCCS provided support. This exacerbated some of the challenges agencies have encountered.

EXAMPLES OF AGENCY, LOCAL AND STATE STRATEGIES

Agencies have implemented an initial strategy of executing the low hanging fruit. Services they have moved to the cloud have primarily been email, web services, and collaboration software while they determine how to handle more difficult applications. Several agencies such as DISA and the Postal Service have made progress with data center consolidation while DHS and DoS are in the middle of significant data center consolidations. Smaller agencies who can't afford changes are making small server room consolidations and adopting virtualization and cloud computing services. For cloud implementation, most agencies seem to be implementing private clouds such as DISA, Department of State (DOS), Department of Energy (DOE), and DHS. Some such as the Army and Small Business Administration (SBA) are using mixed solutions, and others such as Agriculture have turned to public providers.

DISA is implementing a private cloud for DOD providing web content and application delivery, voice switching, and other capabilities. It implemented a Demilitarized Zone (DMZ) between its private cloud enterprise and the Internet through 11 entry points. The Air Force and the Army are already utilizing DISA for some applications and the Army is now migrating email services to them.[148] The Army is using a combination of its own private cloud and outsourcing some services to DISA. It is consolidating down to two Area Processing Centers (APC). It implemented a moratorium on purchasing new servers and voice switches and intends to pay for the new APCs through savings from the moratorium.[149]

DOS is implementing a private cloud. It is consolidating from 11 data centers down to two. GSA similarly is consolidating from 13 to 3 data centers by 2015.

DOE has been consolidating for several years in their private cloud by moving their 89 smaller data centers into two primary data centers. Through virtualization and reducing applications they have reduced servers from 200 to 100 in the two main facilities.[150]

DHS is an example of a Department that intends to keep their services in house using a private cloud but is using vendors to run the cloud for them in some locations. They migrated email to the private cloud and by 2014 should complete their data center consolidation from 24 down to two. One will be managed by Computer Science Corp and the other by Hewlett-Packard.[151] By the end of 2011 DHS expects to have consolidated functions from Customs and Border Protection and Immigration and Customs Enforcement. Because some of their agencies such as the Federal Emergency Management Agency and Citizen and Immigration Services are public facing, they will likely transition to a mixed capability with most of the Department private but a few subordinate agencies on public clouds.[152]

The SBA is also implementing a mixed solution of primarily a private cloud with some outsourcing. Their biggest consolidation effort has been in virtualization. Their consolidation has been mostly on the application side shrinking 60 client record apps down to 14 and moving apps from old Cobol based programs to Oracle and Microsoft platforms.[153] This is an example of streamlining business practices because of moving to the cloud.

Examples of agencies using public clouds are the Dep. of Agriculture which is moving email, document sharing, and collaboration to Microsoft's cloud infrastructure and GSA which moved email to Google Apps for Government.[154] GSA is also moving some of their apps to the cloud including their USA.gov, Data.gov, challenge.gov and their Citizen's Engagement Platform. Their Center for New Media and Citizen Engagement allows government agencies to deploy tools such as blogs, wikis, and forums to help engage the public in a simple, cost effective way. These tools are based on open source coding to make them widely shareable.[155]

It is paramount that agencies transitioning to a public cloud understand where their data is stored and processed and identifies this in their Statement of Agreement with the provider. If it goes through another country, it could be subject to their laws, regulations, and access. This is not acceptable for some government held information. Agencies must also keep their users in mind while implementing a transition. In many instances, consolidations mean less local administrative control and user assistance and needs could easily be lost in the ambiguity of the cloud. One recommendation is consultant services can be of great assistance to an agency transitioning from their own systems to a public cloud. Typical IT sections have neither the experience nor personnel they can dedicate to interfacing with the provider while simultaneously trying to maintain current operational capabilities until the migration is complete. Insufficient planning or interoperability preparations with the provider can have disastrous results during a migration.

Several of the federal government's biggest computing consumers are expanding their mission set to provide services to other agencies that can't afford their own. Examples are DISA, the Interior Department's National Business Center (NBC), and NASA. These agencies already possess the infrastructure to provide network, IT and acquisition services.[156] This also positions cloud service providers inside the federal firewall. DISA and DHS are already providing services for internal agencies and offices. NBC is providing collaboration, social media services, infrastructure and tool development services; especially in the areas of financial management, human resources, acquisition and other enterprise applications.[157]

States, counties, and municipalities are all looking at consolidation and reducing IT costs just like the federal government. It could be argued that saving on IT may be even more important at the state level due to constitutionally mandated balanced budgets and the significant deficits many states have. According to Utah CIO Stephen Fletcher Utah, Michigan, and Colorado are doing the most to reduce data centers and migrate to cloud computing. Utah has reduced data centers from 35 to 2 and from 1800 to 450 servers of which 75% are virtualized. The state then offers data center services to its cities and counties who can pay for their services out of their operational budgets. It precludes smaller cities from having to invest in upfront costs.[158]

A few large municipalities have taken steps to move to the cloud. Although big cities have a large enough employee base to implement specific cloud scenarios for themselves, most should consider a public cloud with an established provider as long as they can ensure privacy and security of their constituents' data. Los Angeles moved its email system to the Google cloud; and New York is working with Microsoft cloud computing with estimated savings of over $50 million over 5 years.[159] For the smaller towns and counties, it makes sense to take advantage of capabilities provided by their states or the federal government.

Appendix D – Social Networking

Porter's Five Forces: Social Networking

Five Forces	Assessment
Supplier Power	High: visitors drive subscriptions/advertising revenues Lower for larger SN businesses like Facebook
Buyer Power	High: substitutes SN options/low switching costs
Threat of new entrants	High: low barriers to entry, access to inputs
Threat of substitutes	High: numerous, low switching costs
Rivalry	High: low exit barriers, strong growth, product differentiation

Figure 1: Porter Five Forces analysis, source: "Social Networking as a New Trend in a e-Marketing", T. Andrew Yang and Dan J. Kim.

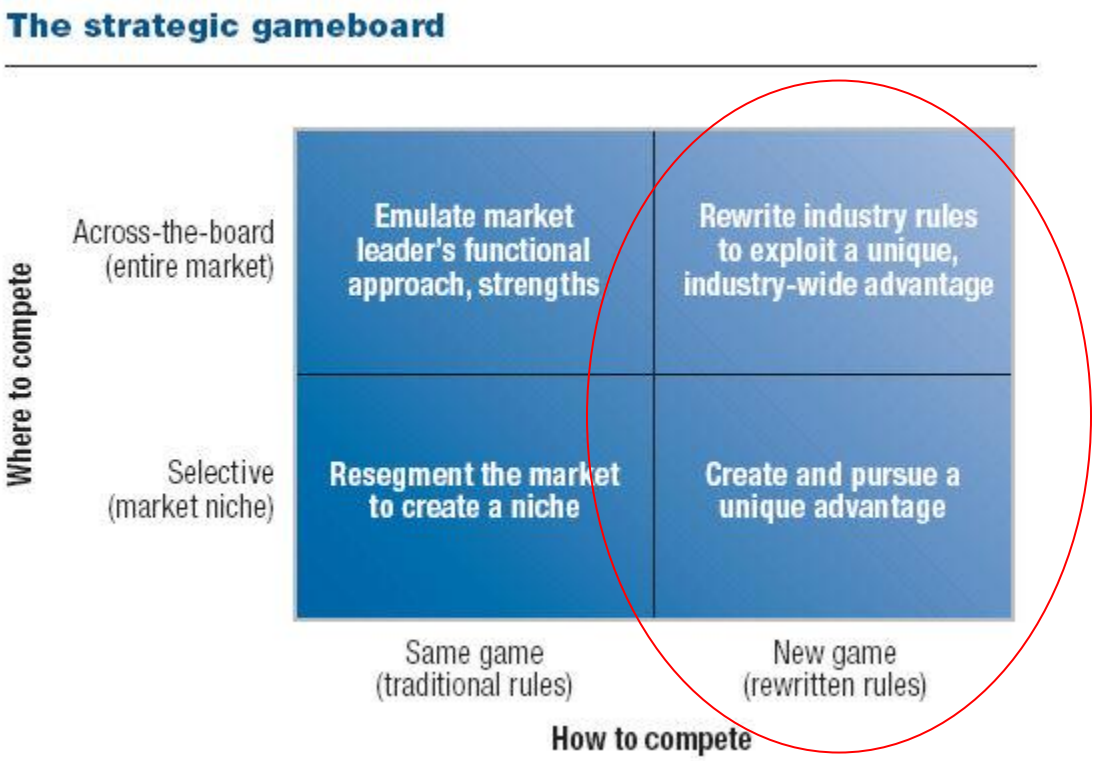

Figure 2: Strategic Gameboard, source: New-Game Strategies, McKinsey Classic by Roberto Buaron, ~1980

ENDNOTES

[1] Nicholas G. Carr, *The Big Switch: Rewiring the World, from Edison to Google*, (New York: W.W. Norton & Co, 2008), 15.

[2] Casey Thormahlen, "IBISWorld Industry Report 51419a: Internet Service Providers in the US," November 2010, 44, http://www.ibisworld.com/industryus/default.aspx?indid=1901.

[3] Casey Thormahlen, "IBISWorld Industry Report 51331a: Voice Over Internet Protocol Providers (VoIP) in the US," February 2011, 41, http://www.ibisworld.com/industryus/default.aspx?indid=1901.

[4] Agata Kaczanowska, "IBISWorld Industry Report 51322: Cable, Internet & Telephone Providers in the US," December 2010, 19, http://www.ibisworld.com/industryus/default.aspx?indid=1264.

[5] CTIA - The Wireless Association. "Wireless In America." *CTIA Wireless In America*, http://files.ctia.org/pdf/HowWirelessWorks_jan2011.pdf, January 27, 2011

[6] Robert Roche, "Wireless in the U.S.: A Snapshot." Lecture, A Presentation to the ICAF from CTIA - The Wireless Association, Washington, D.C., February 24, 2011.

[7] James Moorman, "Telecommunications: Wireless." *S&P Netadvantage*, www.netadvantage.standardandpoors.com/NASApp/NetAdvantage/showIndustrySurvey.do?cod=tws, February 19, 2011.

[8] Casey Thormahlen, " IBISWorld Industry Report 51332: Wireless Telecommunications Carriers in the US," www.ibisworld.com/industryus/ default.aspx?indid=1267, 31, February 23, 2011.

[9] Ibid., 19.

[10] Ibid., 21.

[11] Rob Cross and Andrew Parker, *The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations*, (Boston: Harvard Business School Press, 2004), 10.

[12] Chris Codella, Ph.D, "IBM Research," GTO presentation to ICAF ICT Seminar, March 8, 2011.

[13] Casey Thormahlen, "Internet Publishing and Broadcasting in the US", http://www.ibisworld.com/industryus/default.aspx?indid=1974, February 2011.

[14] Devi Gnyawali, Weiguo and James Penner, *Competitive Actions and Dynamics in the Digital Age: An Empirical Investigation of Social Networking Firms,* Information Systems Research, volume 21, number 3 (2010), 595-596.

[15] Mary Meeker, Scott Devitt, and Liang Wu, "Internet Trends," http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, *Morgan Stanley powerpoint brief*, April 12, 2010, 30.

[16] Casey Thormahlen, "Internet Publishing and Broadcasting in the US", http://www.ibisworld.com/industryus/default.aspx?indid=1974, February 2011.

[17] Mary Meeker, Scott Devitt, and Liang Wu, "Internet Trends," http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, *Morgan Stanley powerpoint brief*, April 12, 2010, 30.

[18] R. Dai, "IBIS World Industry Report 54151: IT Consulting in the U.S.," http://www.ibisworld.com/industryus/default.aspx?indid=1415 November 2010, 3.

[19] Casey Thormahlen, "IBIS World Industry Report 51121: Software Publishing in the U.S.," http://www.ibisworld.com/industryus/default.aspx?indid=1239 February 2011, 5.

[20] Ibid., 5.

[21] Ibid., 7.

[22] Ibid., 4.

[23] Agata Kaczanowska, "IBISWorld Industry Report 51322: Cable, Internet & Telephone Providers in the US," http://www.ibisworld.com/industryus/default.aspx?indid=1264 December 2010, 19.

[24] Ibid., 18.

[25] Casey Thormahlen, "IBISWorld Industry Report 51331b: Wired Telecommunications Carriers in the US," February 2011, 4, http://www.ibisworld.com/industryus/default.aspx?indid=1268.

[26] Ibid., 36.

[27] Kaczanowska, 19.

[28] Todd Rosenbluth, "Standard and Poor's: Industry Surveys, Telecommunications: Wireline," September 23, 2010, 3, http://www.netadvantage.standardandpoors.com/NASApp/NetAdvantage/showIndustrySurveyPDF.do?loadIndSurFromMenu=pdf. 8.

[29] Casey Thormahlen. "IBISWorld Industry Report 33411b: Computer Monitor & Peripheral Manufacturing in the US." February, 2011, 6, http://www.ibisworld.com/industryus/default.aspx?indid=741 .

[30] Casey Thormahlen. "IBISWorld Industry Report 33421: Telecommunication Networking Equipment Manufacturing in the US." February 2011, 20, http://www.ibisworld.com/industryus/default.aspx?indid=745.

[31] Casey Thormahlen. "IBISWorld Industry Report 33411a: Computer Manufacturing in the US." February 2011, 22, http://www.ibisworld.com/industryus/default.aspx?indid=740

[32] Stephen Ezell, Scott Andes, "ICT R&D Policies: An International Perspective," *IEEE Internet Computing*, (July 2010, Vol. 14, Issue: 4): 78.

[33] President's Council of Advisors on Science and Technology. "Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology." Executive Office of the President. www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf (accessed April 29, 2011).

[34] Barry Jaruzelski and Kevin Dehoff, "The Global Innovation 1000: How the Top Innovators Keep Winning," *Strategy and Business* (New York, NY: Booz & Company, Issue 61, Winter 2010): 1.

[35] Ibid., 7.

[36] OECD (2010), "OECD Information Technology Outlook 2010," 170, OECD Publishing. http://dx.doi.org/10.1787/it_outlook-2010-en.

[37] OSTP Letter, "Innovation, Education, Infrastructure: Science, Technology, STEM Education, and 21st Century Infrastructure in the 2012 Budget," 5 (Office of Science and Technology Policy, Executive Office of the President, February 14, 2011). http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-rd-fs.pdf.

[38] Ezell and Andes, 76.

[39] Daniel Karnis, "Navigating the R&D Tax Credit," *Journal of Accountancy* (March 2010), http://www.journalofaccountancy.com/Issues/2010/Mar/20092122.

[40] STP Letter, "Innovation, Education, Infrastructure: Science, Technology, STEM Education, and 21st Century Infrastructure in the 2012 Budget," 3 (Office of Science and Technology Policy, Executive Office of the President, February 14, 2011). http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-rd-fs.pdf.

[41] Anne-Marie Lasowski, Director, Acquisition and Sourcing Management, U.S. Government Accountability Office, "Export Controls: Fundamental Reexamination of System Is Needed to Help Protect Critical Technologies," *Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives,* June 4, 2009, GAO-09-767T, http://www.exportcontrols.msu.edu/docs/GAO_Export_Controls_Fundamentals.pdf, 0.

[42] United States Department of State, Directorate of Defense Trade Controls, "Commodity Jurisdiction," http://pmddtc.state.gov/commodity_jurisdiction/index.html, March 27, 2011.

[43] Anne-Marie Lasowski, Director, Acquisition and Sourcing Management, U.S. Government Accountability Office, "Export Controls: Fundamental Reexamination of System Is Needed to Help Protect Critical Technologies," *Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives,* June 4, 2009, GAO-09-767T, http://www.exportcontrols.msu.edu/docs/GAO_Export_Controls_Fundamentals.pdf, 4.

[44] Ministry of Commerce & Industry, "Total Trade Data: Export Import Data Bank of India," Government of India, http://commerce.nic.in/eidb/iecnttopnq.asp , March 28, 2011.

[45] Mark Drapeau and Linton Wells III, "Social Software and National Security: An Initial Net Assessment," *Center for Technology and National Security Policy,* April 2009, V.

[46] Ibid.

[47] Daniel T. Kuehl, and Robert A. Miller, "Cyberspace and the 'First Battle' in 21st-century War," *Defense Horizons* 68, September 2009, 2.

[48] Randy Reichart, "Moore's Law and the Pace of Change,"*Internet Reference Services Quarterly,* 11.3 (2006): 117-124.

[49] Lewis Jacobsen, "Barack Obama In State of Union Says U.S. Corporate Tax Rate Is Among The World's Highest," *St Petersburg Times Politifact Section,* Jan 25, 2011, http://www.politifact.com/truth-o-meter/statements/2011/jan/25/barack-obama/barack-obama-state-union-says-us-corporate-tax-rat/, April 18, 2011.

[50] "2010 Africa - Fixed-line Telecommunications and Infrastructure Statistics, Executive Summary," *BuddeComm,* http://www.budde.com.au/Research/2010-Africa-Fixed-line-Telecommunications-and-Infrastructure-Statistics-tables-only.html, May 16, 2011.

[51] "Submarine cable trial lights path to greater capacity for global networks," *Webwire* March 10, 2011, http://www.webwire.com/ViewPressRel.asp?aId=133656, April 18, 2011.

[52] Richard Waters, "Technology: A Dip in the Valley," *Financial Times*, January 19 2011, http://www.ft.com/intl/cms/s/0/33902778-2405-11e0-bef0-00144feab49a.html#axzz1MiUQy9yJ, January 22, 2011.

[53] Tim Berners-Lee, James Hendler, and Ora Lasilla, "The Semantic Web: A New Form of Web Content that is Meaningful to Computers will Unleash a Revolution of New Possibilities," *Scientific American*, May 17, 2001, http://www.scientificamerican.com/article.cfm?id=the-semantic-web&print=true, March 26, 2011.

[54] Ellen Messemer, "Open Source Software a Security Risk," *CIO*, July 21, 2008, http://www.cio.com/article/438728/Open_Source_Software_a_Security_Risk, March 26, 2011.

[55] China National Bureau of Statistics, Statistical Communiqué of the People's Republic of China on the 2010 National Economic and Social Development, February 28, 2011, http://www.stats.gov.cn/was40/gjtjj_en_detail.jsp?searchword=internet&channelid=9528&record=1, May 16, 2011.

[56] China National Bureau of Statistics, "Statistical Communiqué of the People's Republic of China on the 2007 National Economic and Social Development," February 28, 2008, http://www.stats.gov.cn/was40/gjtjj_en_detail.jsp?searchword=internet&channelid=9528&record=4, May 16, 2011.

[57] OSTP Letter, "Innovation, Education, Infrastructure: Science, Technology, STEM Education, and 21st Century Infrastructure in the 2012 Budget," 5 (Office of Science and Technology Policy, Executive Office of the President, February 14, 2011). http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY12-rd-fs.pdf

[58] Ibid., 9.

[59]Todd Rosenbluth, "Standard and Poor's: Industry Surveys, Telecommunications: Wireline," September 23, 2010, 7, http://www.netadvantage.standardandpoors.com/NASApp/NetAdvantage/showIndustrySurveyPDF.do?loadIndSurFromMenu=pdf.

[60] John Levine and Michael Hogg, *Encyclopedia of Group Processes and Intergroup Relations* (London: SAGE Reference Publishing, 2010), 817, http://www.andrew.cmu.edu/user/krack/documents/pubs/2010/2010KrackhardtEncyclopedia.pdf.

[61] Mark Suster, "Social Networking: The Past," *Tech Crunch*, December 10, 2010 http://techcrunch.com/2010/12/03/social-networking-past.

[62] Casey Thormahlen, "Internet Publishing and Broadcasting in the US", http://www.ibisworld.com/industryus/default.aspx?indid=1974, February 2011.

[63] Devi Gnyawali, Weiguo and James Penner, "Competitive Actions and Dynamics in the Digital Age: An Empirical Investigation of Social Networking Firms," *Information Systems Research*, 21:3 (2010): 595-596.

[64] Casey Thormahlen, "Internet Publishing and Broadcasting in the US", http://www.ibisworld.com/industryus/default.aspx?indid=1974, February 2011.

[65] Devi Gnyawali, Weiguo and James Penner, "Competitive Actions and Dynamics in the Digital Age: An Empirical Investigation of Social Networking Firms," *Information Systems Research*, 21:3 (2010): 595-596.

[66] Mary Meeker, Scott Devitt, and Liang Wu, "Internet Trends," http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, *Morgan Stanley Powerpoint Brief*, April 12, 2010, 30.

[67] Ibid.

[68] Ibid.

[69] David Singh Grewal, *Network Power: The Social Dynamics of Globalization*, (New Haven: Yale University Press, 2008), 17-20.

[70] Chris Codella, Ph.D., "IBM Research GTO," presentation to ICAF ICT Seminar, March 8, 2011.

[71] Judith Lamont, Ph.D. "Social networking helps sustain innovation," *KMWorld*, May 28, 2010, http://www.kmworld.com/Articles/Editorial/Feature/Social-networking-helps-sustain-innovation-67347.aspx.

[72] Mike Brown, "30 Ideas for Using Social Networks to Help You Be More Innovative", *Blogging Innovation*, April 26, 2010, http://www.business-strategy-innovation.com/wordpress/2010/04/innovation-perspectives, February 24, 2011.

[73] Rob Cross and Andrew Parker, *The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations*, (Boston: Harvard Business School Press, 2004); 10

[74] Chris Codella, Ph.D, "IBM Research GTO," presentation to ICAF ICT Seminar, March 8, 2011.

[75] Sharon Gaudin, "Study: Facebook use cuts productivity at work," *Computer World*, July 22, 2009, http://www.computerworld.com/s/article/9135795/Study_Facebook_use_cuts_productivity_at_work.

[76] Rich Bowden, "Web surfing increases Productivity," *The Tech Herald*, April 6, 2009, http://www.thetechherald.com/article.php/200915/3374/Study-finds-workplace-web-surfing-increases-productivity**.**

[77] "European Study Reveals: Social Networking Increases Productivity," *Geek with Laptop*, November 12, 2008, http://www.geekwithlaptop.com/european-study-reveals-social-networking-increases-productivity.

[78] Ibid.

[79] Jim Tobin,"Top 50 Branded Facebook Fan Pages, February 2011," *Ignite Social Media*, http://www.ignitesocialmedia.com/facebook-marketing/ , February 24, 2011.

[80] Mary Meeker, Scott Devitt, and Liang Wu, "Internet Trends," *Morgan Stanley Powerpoint Brief*, April 12, 2010, 12, http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf.

[81] Sara Underwood, "Social Network Savings," *My Fox Boston*, www.myfoxboston.com/dpp/news/special_reports/Social_Network_Savings, February 26, 2011.

[82] "A world of connections," *The Economist*: *A Special Report on Social Networking*, January 30, 2010, 3-4, http://www.economist.com/node/15351002?story_id=15351002&source=hptextfeature.

[83] Ibid., 3.

[84] Sampad Swain, "Social Network Monetization – Deeper Insights," May 26, 2009, http://sampadswain.com/2009/05/social-network-monetization-deeper-insights/#, March 13, 2010.

[85] S. Craig Watkins, *The Young and the Digital: What the Migration to Social-Network Sites, Games, and Anytime, Anywhere Media Means for Our Future*, (Boston: Beacon Press, 2009), 68-69.

[86] Clay Shirky. "The Political Power of Social Media," *Foreign Affairs*, January/February 2011, 35-36.

[87] Ibid.

[88] Ibid, 197.

[89] Mary Meeker, Scott Devitt, and Liang Wu, "Internet Trends," http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf, *Morgan Stanley Powerpoint Brief*, April 12, 2010, 7-12.

[90] Mark Suster, "Social Networking: The Past" *Tech Crunch*, December 5, 2010, http://techcrunch.com/2010/12/03/social-networking-future.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Mark Drapeau and Linton Wells III, "Social Software and National Security: An Initial Net Assessment," *Center for Technology and National Security Policy*, April 2009, V.

[95] Ibid.

[96] Vivek Kundra, "Federal Cloud Computing Strategy," US CIO, February 2011, 1. http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[97] Vivek Kundra, "Memorandum for Chief Information Officers, Subject: Federal Data Center Consolidation Initiative," February 26, 2010, 1, http://www.cio.gov/documents/federal-data-center-consolidation-initiative-02-26-2010.pdf.

[98] Ibid.

[99] Ibid., 2.

[100] Vivek Kundra, "25 Point Implementation Plan to Reform Federal Information Technology Management, US CIO, December 2010; 1 http://www.cio.gov/documents/25-point-implementation-plan-10-10-2010.pdf.

[101] Ibid.,1.

[102] Vivek Kundra, "Federal Cloud Computing Strategy" US CIO, February 2011;1 http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[103] Ibid., 2.

[104] Ibid., 3.

[105] Rutrell Yasin, "Data Center Consolidation a Decade Away, Report Says", *Government Computer News*, September 2010; 1, http://gcn.com/articles/2010/09/23/INPUT-data-center-consolidation-Report.aspx?p=1, February 12, 2011.

[106] Rutrell Yasin, "5 Steps to Secure Your Data Center," *Government Computer News*, November 2009; 1, http://gcn.com/articles/2009/11/30/5-steps-to-a-secure-data-center.aspx?p=1, February 10, 2011.

[107] INPUT Industry Report, "Assessment of the 2010 Federal Data Center Consolidation Initiative," *Deltek Information Solutions*, September 2010; 1 http://www.input.com/corp/library/detail.cfm?itemID=13352&cmp=ILC-pubsitecarouseldc, March 7, 2011.

[108] Ibid.

[109] Stuart Henderson, Salina Lin, Maurice Soloman, and Chris Hines, "The Wisdom of the Cloud," *IBM Institute for Business Value,* November 2010, 10.

[110] Ibid.

[111] "Virtualization and Cloud Technologies Add Complexity to Disaster Recovery Initiatives", *Symantec Corp*., November, 2010, 1, www.symantec.com. 15 Feb, 2011

[112] Ibid.

[113] Anderie Traian, "Cloud Computing Challenges and Related Security Issues, A Survey Paper," April 30, 2009, 9, http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html, November 24, 2010.

[114] Stuart Henderson, Salina Lin, Maurice Soloman, and Chris Hines, "The Wisdom of the Cloud," *IBM Institute for Business Value,* November 2010, 1.

[115] Ibid., 6.

[116] Ibid., 5.

[117] "Technology and the Advent of Cyberwar," *Information Security Resources (Online)*, December 15, 2009, http://information-security-resources.com/2009/12/15/technology-and-the-advent-of-cyber-war, March 12, 2011.

[118] "Emerging Cyber Threats Report 2011," *Georgia Tech Information Security Center* (GTISC), 4, http://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf, February 18, 2011.

[119] "10 Conservative Principles for Cybersecurity Policy," *Backgrounder*, The Heritage Foundation, January 31, 2011, 5. http://www.heritage.org/Research/Reports/2011/01/10-Conservative-Principles-for-Cybersecurity-Policy

[120] "Study: Cybercrime cost firms $1 trillion globally," *CNET News Online*, January 28, 2009, http://news.cnet.com/ 8301-1009_3-10152246-83.html?part=rss&subj=news&tag=2547-1_3-0-20 , February 27, 2011.

[121] Georgia Tech Information Security Center (GTISC), 6.

[122] "McAfee Threats Report: Second Quarter 2010," *McAfee Labs*, http://www.mcafee.com/us/local_content/ reports/q22010_threats_report_en.pdf, February 18, 2011.

[123] Georgia Tech Information Security Center (GTISC), 6.

[124] Georgia Tech Information Security Center (GTISC), 8.

[125] Ibid., 4.

[126] Adam Barth, Collin Jackson, Charles Reis, and The Google Chrome Team, "The Security Architecture of the Chromium Browser," *Technical Report 2008*, http://seclab.stanford.edu/websec/chromium/chromium-security-architecture.pdf.

[127] "'Identity Ecosystem' to replace passwords, draft strategy suggests," *Federal Computer Week (Online)*, 25 June 2010, http://fcw.com/articles/2010/06/25/national-strategy-for-trusted-identities-in-cyberspace.aspx, March 12, 2011.

[128] Stewart Baker, Shaun Waterman, and George Ivanov, McAfee. "In the Crossfire: Critical Infrastructure in the Age of Cyber War," *Center for Strategic and International Studies*, (2010), 27.

[129] Ibid, 14.

[130] North American Industry Classification System, http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2007, February 3, 2011.

[131] Vivek Kundra, "Federal Cloud Computing Strategy" US CIO, (February 2011); 5 http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[132] J. Rittinghouse, and J. Ransome**,** *Cloud Computing: Implementation, Management, and Security* (Boca Raton: CRC Press, 2010), xxvi; 50

[133] "Hypervisors," *EEMBC,* http://www.eembc.org/benchmark/hyper_sl.php March 26, 2011.

[134] Vivek Kundra, "Federal Cloud Computing Strategy," US CIO, (February 2011); 5 http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[135] Vivek Kundra, "Federal Data Center Consolidation Initiative". US CIO, (February, 2010); 1, http://www.cio.gov/documents/federal-data-center-consolidation-initiative-02-26-2010.pdf

[136] Vivek Kundra, "Federal Cloud Computing Strategy" US CIO, (February 2011); 32 http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[137] David McClure, Dr., "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 2, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

[138] Vivek Kundra, "Federal Cloud Computing Strategy" US CIO, (February 2011); 25 http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[139] Ibid., 28.

[140] Rutrell Yasin, "Agencies, Choose Your Clouds-Here Are 3 Basic Options," *Government Computer News, (*February 2011), 2. http://gcn.com/articles/2011/02/07/Feature-cloud-sourcing.aspx?p=1. 5 Feb, 2011

[141] David McClure, Dr., "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 3, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

[142] Vivek Kundra, "Federal Cloud Computing Strategy" US CIO, (February 2011); 27. http://www.cio.gov/documents/federal-cloud-computing-strategy 02-10-2011.pdf.

[143] Ibid., 27.

[144] David McClure, Dr., "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 4, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

.

[145] Vivek Kundra, "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 1, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

[146] Vivek Kundra, "25 Point Implementation Plan to Reform Federal Information Technology Management, US CIO, (December 2010); 1 http://www.cio.gov/documents/25-point-implementation-plan-10-10-2010.pdf.

[147] Vivek Kundra, "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 3, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

[148] Rutrell Yasin, "Agencies, Choose Your Clouds-Here Are 3 Basic Options," *Government Computer News, (*February 2011); 2. http://gcn.com/articles/2011/02/07/Feature-cloud-sourcing.aspx?p=1, February 5, 2011.

[149] Amber Corrin, "Army Steps Up Data Center Consolidation After Imposing Server Moratorium," *Government Computer News,* (June 2010), 1, http://gcn.com/articles/2010/06/10/Army-server-moratorium.aspx?p=1, February 10, 2011.

[150] Rutrell Yasin, "After Data Center Consolidation, Beware Legacy Apps," *Government Computer News,* (January 2011), 2, http://gcn.com/articles/2011/01/14/afcea-data-center-consolidation.aspx?p=1, February 12, 2011.

[151] Rutrell Yasin, "DHS Offers E-mail Services Via Private Cloud," *Government Computer News,* (August 2010), 1, http://gcn.com/articles/2010/08/31/Richard-Spires-DHS-Data-Center-Consolidation.aspx?p=1, February 5, 2011.

[152] Rutrell Yasin, "After Data Center Consolidation, Beware Legacy Apps," *Government Computer News,* (January 2011), 2, http://gcn.com/articles/2011/01/14/afcea-data-center-consolidation.aspx?p=1, February 12, 2011.

[153] Rutrell Yasin, "The Political Hurdle to Data Center Consolidation," *Government Computer News,* (June 2010), 2, http://gcn.com/articles/2010/06/08/data-center-consolidation.aspx?p=1, February 5, 2011.

[154] Rutrell Yasin, "Agencies, Choose Your Clouds-Here Are 3 Basic Options," *Government Computer News,* (February 2011), 2, http://gcn.com/articles/2011/02/07/Feature-cloud-sourcing.aspx?p=1, February 5, 2011.

[155] David McClure, Dr. "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology," *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs,* April 12, 2011, 9, http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

[156] Rutrell Yasin, "Agencies, Choose Your Clouds-Here Are 3 Basic Options," *Government Computer News,* (February 2011), 2, http://gcn.com/articles/2011/02/07/Feature-cloud-sourcing.aspx?p=1, February 5, 2011.

[157] Rutrell Yasin, "Federal Agencies in the Cloud," *Government Computer News*, (February 2011), 2, http://gcn.com/articles/2011/02/07/Feature-Cloud-Sourcing-agency-list.aspx?p=1, February 5, 2011.

[158] Rutrell Yasin, "State IT Diet: Consolidation, Cloud, and Shared Services," *Government Computer News*, (February 2011), 2, http://gcn.com/articles/2011/02/07/Federal-Cloud-Sourcing-Side-1.aspx?p=1, February 5, 2011.

[159] Ibid.

Bibliography

"Alphabetical Index to the Commerce Control List." http://www.bis.doc.gov/policiesandregulations/ccl_index.pdf.

"Assessment of the 2010 Federal Data Center Consolidation Initiative." *INPUT Industry Report, Deltek Information Solutions* 1-2 (Sep 2010). http://www.input.com/corp/library/detail.cfm?itemID=13352&cmp=ILC-pubsitecarouseldc

Atkinson, Robert D. and Daniel D. Castro. "Digital Quality of Life Understanding the Personal & Social Benefits of the Information Technology Revolution [Understanding the personal & social benefits of the information technology revolution.]" Washington, D.C: Information Technology and Innovation Foundation, 2008. http://www.itif.org/files/DQOL.pdf; http://www.itif.org/files/DQOL.pdf ed.

Atkinson, Dr. Robert D. "The Globalization of R&D and Innovation: How Do Companies Choose Where to Build R&D Facilities?" *Testimony before the U.S. House of Representatives Committee on Science and Technology Subcommittee on Technology and Innovation* (October 4, 2007). http://www.itif.org/files/AtkinsonHouseRDOffshoreTestimony.pdf

Atkinson, Robert D. & Andrew S. McKay. "Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution." Washington, DC: The Information Technology & Innovation Foundation, March 2007.

Baker, Stewart, Shaun Waterman, and George Ivanov, McAfee. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. Santa Clara, CA: Center for Strategic and International Studies.

Barth, Adam, Jackson, Collin, Reis, Charles, and The Google Chrome Team. *The Security Architecture of the Chromium Browser*, Technical Report 2008.

Berners-Lee, Tim, Hendler, James, and Ora Lasilla. "The Semantic Web: A New Form of Web Content that is Meaningful to Computers will Unleash a Revolution of New Possibilities," *Scientific American* (May 17, 2001). http://www.scientificamerican.com/article.cfm?id=the-semantic-web&print=true.

Binning, David "Top Five Cloud Computing Security Issues". *ComputerWeekly.com* (24 April, 2009). http://computerweekly.com/articles/2010/01/12/235782/Top-five-cloud-computing

Brown, Mike, "30 Ideas for Using Social Networks to Help You Be More Innovative," *Blogging Innovation* (April 26, 2010). http://www.business-strategy-innovation.com/wordpress/2010/04/innovation-perspectives.

Bowden, Rich. "Web surfing increases Productivity," *The Tech Herald* (April 6, 2009).

Bureau of Labor Statistics, "Career Guide to Industries, 2010-2011 Edition, Computer and Electronic Product Manufacturing." http://www.bls.gov/oco/cg/cgs010.htm.

Carr, Nicholas G. *The Big Switch: Rewiring the World, from Edison to Google*. 1st ed. New York: W.W. Norton & Co, 2008.

Chabrow, Eric. "White House Issues Secure Cloud Computing Guidance FedRAMP Requirements Aimed to Easy Cloud Computing Adoption." *GovInfoSecurity* (2 November 2010). http://www.govinfosecurity.com

China National Bureau of Statistics. "Statistical Communiqué of the People's Republic of China on the 2010 National Economic and Social Development." (February 28, 2011). http://www.stats.gov.cn/was40/gjtjj_en_detail.jsp?searchword=internet&channelid=9528&record=1.

China National Bureau of Statistics. "Statistical Communiqué of the People's Republic of China on the 2007 National Economic and Social Development." (February 28, 2008). http://www.stats.gov.cn/was40/gjtjj_en_detail.jsp?searchword=internet&channelid=9528&record=4.

"Cloud Computing Moves Into New Growth Phase." *Investors.com*. http://www.investors.com/NewsAndAnalysis/Article/567353/201103281818/Cloud-Based-Software-Sky-High.htm.

Collins, Jim. *Good to Great*. New York, NY: HarperCollins Publishers, Inc., 2001.

"Computer Hardware in the United States." *DATAMONITOR* (June 2010).

Corrin, Amber. "Army Steps Up Data Center Consolidation After Imposing Server Moratorium". *Government Computer News* (June 2010). http://gcn.com/articles/2010/06/10/Army-server-moratorium.aspx?p=1.

Covington & Burling LLP, "U.S. Export Control Reform Developments," *E-Alert, Foreign Trade Controls (*December 16, 2010). http://www.cov.com/files/Publication/c94619bc-161f-4184-8f37-6de6f15c75ca/Presentation/PublicationAttachment/ab168727-9c9d-4ef1-a6ea-70f10c75a370/U.S.%20Export%20Control%20Reform%20Developments.pdf

Cross, Rob and Andrew Parker. *The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations*. Boston, Massachusetts: Harvard Business School Press, 2004.

Dai, R. "IBIS World Industry Report 54151: IT Consulting in the U.S." http://www.ibisworld.com/industryus/default.aspx?indid=1415 November 2010.

Dedrick, Jason and Kraemer, Kenneth L., "Is Production Pulling Knowledge Work to China?" *Computer* (2006).

Defense Information Systems Agency (DISA). “DISA Campaign Plan.” (2010). http://www.disa.mil/computing/cloud/index.html

"Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology." *Executive Office of the President, President's Council of Advisors on Science and Technology*. www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf .

Drapeau, Mark and Linton Wells III. “Social Software and National Security: An Initial Net Assessment.” *Center for Technology and National Security Policy* (April 2009): V.

Drucker, Jesse. “Dodging Repatriation Tax Lets U.S. Companies Bring Home Cash.” *Bloomberg* (December 29, 2010). http://www.bloomberg.com/news/2010-12-29/dodging-repatriation-tax-lets-u-s-companies-bring-home-cash.html

“Emerging Cyber Threats Report 2011.” Georgia Tech Information Security Center (GTISC). http://www.gtisc.gatech.edu/pdf/cyberThreatReport2011.pdf.

EPIC – Cloud Computing. Electronic Privacy Information Center (EPIC).org http://epic.org/privacy/cloudcomputing/.

Executive Order 13558 – Expert Coordination Enforcement Center. (November 9, 2010). http://www.whitehouse.gov/the-press-office/2010/11/09/executive-order-export-coordination-enforcement-center

Ezell, Stephen and Scott Andes, “ICT R&D Policies: An International Perspective,” *IEEE Internet Computing* 14, no.4 (July 2010).

Ezell, Stephen and Scott Andes. “Public Policy: Country Intensity.” *IEEE Internet Computing Web Extra.* Information Technology and Innovation Foundation (2010). http://www.computer.org/cms/Computer.org/dl/mags/ic/2010/04/extras/mic2010040076s.pdf.

Fact Sheet on the President's Export Control Reform Initiative. (April 20, 2010). http://www.whitehouse.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative

Federal Register, June 25, 2010, 75 Fed. Reg 36,482, http://edocket.access.gpo.gov/2010/pdf/2010-15072.pdf.

Fergusson, Ian F. “The Export Administration Act: Evolution, Provisions, and Debate,” *Congressional Research Service* (April 26, 2010). http://www.fas.org/sgp/crs/secrecy/RL31832.pdf

Freedberg, Jr., Sydney J. "Biggest Security Threat: Economic Crisis." *NationalJournal.com.* http://security.nationaljournal.com/2009/03/biggest-security-threat-econom.php.

"Gartner: Seven Cloud Computing Security Risks." *InfoWorld*. ,http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0

Gates, Robert M. *Remarks to Business Executives for National Security*, April 20, 2010, http://www.defense.gov/speeches/speech.aspx?speechid=1453 "A world of connections," *The Economist: A Special Report on Social Networking*" (January 30, 2010): 3-4.

Gaudin, Sharon. "Study: Facebook use cuts productivity at work." *Computer World* (July 22, 2009).

Gilder, George. *Computer Industry, The Concise Encyclopedia of Economics*. http://www.econlib.org/library/Enc1/ComputerIndustry.html.

Gnyawali, Devi, Weiguo and James Penner. "Competitive Actions and Dynamics in the Digital Age: An Empirical Investigation of Social Networking Firms." *Information Systems Research* 21, no. 3 (2010): 595-596.

Graham, John R., Michelle Hanlon, and Terry Shevlin. "Barriers to Mobility: The Lockout Effect of U.S. Taxation of Worldwide Corporate Profits." *National Tax Journal* 63, no. 4, Part 2 (December 2010): 1111–1144.

Grewal, David Singh. *Network Power: The Social Dynamics of Globalization*. New Haven: Yale University Press, 2008.

Henderson, Stuart and Salina Lin, and Maurice Soloman, and Chris Hines. "The wisdom of the Cloud". *IBM Institute for Business Value* (November 2010): 1-13.

'Identity Ecosystem' to replace passwords, draft strategy suggests." *Federal Computer Week (Online)* (June 25, 2010). http://fcw.com/articles/2010/06/25/national-strategy-for-trusted-identities-in-cyberspace.aspx.

Institute for Defense Analyses. *Export Controls and the Defense Industrial Base.* (January 2007). http://www.acq.osd.mil/ip/docs/ida_study-export_controls_%20us_def_ib.pdf.

Jacobson, Douglas N., Esq. "BIS Takes First Step in Export Control Reform Process by Making Significant Changes to Encryption Export Controls." http://www2.gtlaw.com/practices/GovContracts/pdf/JacobsonEncryptionArticle.doc..

Jaruzelski, Barry and Kevin Dehoff, "The Global Innovation 1000: How the Top Innovators Keep Winning," *strategy+business magazine*, 61 (Winter 2010): 1-14.

Jones, James. *Remarks on The Administrations Export Control Reform Plans*. (June 30, 2010). http://www.aia-aerospace.org/assets/speech_jones_06302010.pdf.

Kaczanowska, Agata, "IBISWorld Industry Report 51322: Cable, Internet & Telephone Providers in the US" (December 2010): 19. http://www.ibisworld.com/industryus/default.aspx?indid=1264.

Karnis, Daniel. "Navigating the R&D Tax Credit." *Journal of Accountancy* (March 2010). http://www.journalofaccountancy.com/Issues/2010/Mar/20092122.

Kelsey, Todd. *Social Networking Spaces: From Facebook to Twitter and Everything in Between*. New York, NY: Springer-Verlag, Inc., 2010.

Krigman, Eliza. "WH Moves Forward with Export Control Reform." *National Journal* (August 30, 2010). http://techdailydose.nationaljournal.com/2010/08/wh-moves-forward-with-export-c.php.

Kundra, Vivek. "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology". *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs*. (12 April, 2011) 1-6. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

Kundra, Vivek. "25 Point Implementation Plan to Reform Federal Information Technology Management. US CIO. 1-40. (December 2010).

Kundra, Vivek. "Federal Cloud Computing Strategy" US CIO. 1-39. (February 2011).

Kundra, Vivek. "Federal Data Center Consolidation Initiative". US CIO. 1-2 (February, 2010). http://www.cio.gov/documents/federal-data-center-consolidation-initiative-02-26-2010.pdf.

Lamont, Judith, Ph.D. "Social networking helps sustain innovation" *KMWorld* (May 28, 2010).

Lasowski, Anne-Marie. Director, Acquisition and Sourcing Management, U.S. Government Accountability Office, "Export Controls: Fundamental Reexamination of System Is Needed to Help Protect Critical Technologies." *Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives* (June 4, 2009). GAO-09-767T. http://www.fas.org/programs/ssp/asmp/externalresources/2009/GAOd09767t.pdf

Levine, John and Michael Hogg. *Encyclopedia of Group Processes and Intergroup Relations*. London; SAGE Reference Publishing, 2010. http://www.andrew.cmu.edu/user/krack/documents/pubs/2010/2010KrackhardtEncyclopedia.pdf.

Losman, Donald. "Economic Security: A National Security Folly?" *Policy Analysis*, 409 (2001).

Martin, Belva M. U.S. Government Accountability Office, Report to Senator Jon Kyl, *Export Controls: Agency Actions and Proposed Reform Initiatives May Address Previously Identified Weaknesses, but Challenges Remain*, GAO-11-135R, November 16, 2010, http://www.gao.gov/new.items/d11135r.pdf.

McAfee Threats Report: Second Quarter 2010, McAfee Labs, http://www.mcafee.com/us/local_content/ reports/q22010_threats_report_en.pdf.

McCloskey, Paul. "Gateways to the Cloud-and a Lot More." *Government Computer News* (February 4, 2011): 1-2. http://gcn.com/articles/2011/02/07/Editorial-mobile-computing-IPv6.aspx?p=1.

McClure, David. Dr. "Examining the President's Plan for Eliminating Wasteful Spending in Information Technology". *Testimony Before the Senate Committee on Homeland Security and Governmental Affairs* (12 April, 2011): 1-9. http://hsgac.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_id=8b4a7ea9-6522-48f7-8166-8bf0dbd5595d.

Montgomery, Ken. *Letter to U.S. Department of Commerce, BIS, Regulatory Policy Division, Office of Exporter Services, "Request for Public Comment on Foreign Produced Encryption Items That Are Made From U.S.-Origin Encryption Technology or Software*." (March 9, 2009). http://efoia.bis.doc.gov/pubcomm/records-of-comments/record_of_comments_for_encryption_direct_product_NOI.pdf

Moorman, James. "Telecommunications: Wireless." *S&P Netadvantage*. www.netadvantage.standardandpoors.com/NASApp/NetAdvantage/showIndustrySurvey.do?cod=tws.

Meeker, Mary, Scott Devitt, and Liang Wu. "Internet Trends." *Morgan Stanley Powerpoint Brief* (April 12, 2010). http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf,

Miller, Robert A. and Daniel T. Kuehl. "Cyberspace and the 'First Battle' in 21st-Century War." *Defense Horizons* no. 68 (September, 2009).

Nations, Daniel. "The Top 10 Most Popular Social Networks (2010)." *www.About.com Guide* (March 15, 2010). http://webtrends.about.com/b/2010/03/15/the-top-10-most-popular-social-networks.htm.

North American Industry Classification System. http://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2007.

Obama, Barack H. *National Security Strategy*. Washington, DC: The White House (2010).

Obama, Barack. *Letter From the President to the Speaker of the House of Representatives and the President of the Senate* (August 13, 2009). http://www.whitehouse.gov/the-press-office/letter-regarding-export-administration-act.

Obama, Barack. "Notice of August 12, 2010—Continuation of Emergency Regarding Export Control Regulations," *Federal Register*, Vol 75, Nov.157 (August 16, 2010). http://edocket.access.gpo.gov/2010/pdf/2010-20384.pdf.

Obama, Barack. *Remarks by the President at the Export-Import Bank's Annual Conference* (March 11, 2010).http://www.whitehouse.gov/the-press-office/remarks-president-export-import-banks-annual-conference.

OECD (2010). *OECD Information Technology Outlook 2010*, 43, 170, OECD Publishing. http://dx.doi.org/10.1787/it_outlook-2010-en.

OECD (2010). OECD Information Technology Outlook 2010, 170, OECD Publishing. http://dx.doi.org/10.1787/it_outlook-2010-en.

OSTP Letter. "Innovation, Education, Infrastructure: The FY 2012 Science and Technology R&D Budget," (Office of Science and Technology Policy, Executive Office of the President, February 14, 2011).

OSTP Letter. "Innovation, Education, Infrastructure: Science, Technology, STEM Education, and 21st Century Infrastructure in the 2012 Budget." Office of Science and Technology Policy, Executive Office of the President (2011)

OSTP Letter, "Innovation, Education, Infrastructure: Science, Technology, STEM Education, and 21st Century Infrastructure in the 2012 Budget," 5 (Office of Science and Technology Policy, Executive Office of the President, February 14, 2011).

OUSD(AT&L) Industrial Policy. "Annual Industrial Capabilities Report to Congress." Office of Under Secretary of Defense Acquisition, Technology & Logistics, Industrial Policy (2010).

"Packet Push Powerhouses." *Engineering & Technology* (July 24 – August 6, 2010). http://www.theiet.org./magazine.

Polonsky, Alex S., Esq. "Executive Order Creates Export Coordination Enforcement Center," *Morgan Lewis Publications* (November 22, 2010). http://www.morganlewis.com/index.cfm/fuseaction/publication.print/publicationID/9c67a151-af22-4bb8-9747-7dc8988f4414/.

President Obama Announces First Steps Toward Implementation of New U.S. Export Control System, December 9, 2010, http://www.whitehouse.gov/the-press-office/2010/12/09/president-obama-announces-first-steps-toward-implementation-new-us-expor.

President Obama Lays the Foundation for a New Export Control System to Strengthen National Security and the Competitiveness of Key U.S. Manufacturing and Technology Sectors, August 30, 2010, http://www.whitehouse.gov/the-press-office/2010/08/30/president-obama-lays-foundation-a-new-export-control-system-strengthen-n.

"President Obama's Cybersecurity Initiative Wins Praise." *PCWorld Online* (May 29, 2009). http://www.pcworld.com/article/165773/obamas_cybersecurity_initiative_wins_praise.html.

Qualman, Erik. *Socialnomics: How Social Media Transforms the Way We Live and Do Business*. Hoboken, New Jersey: John Wiley and Sons, Inc.,2009.

"Reducing the Deficit: Spending and Revenue Options," Congressional Budget Office, Pub. No.4212, (2011): 1-2.

Richard Waters, "Technology: A Dip in the Valley," *Financial Times* (January 19 2011). http://www.ft.com/intl/cms/s/0/33902778-2405-11e0-bef0-00144feab49a.html#axzz1MiUQy9yJ.

Roche, Robert. "Wireless in the U.S.: A Snapshot." Lecture, A Presentation to the ICAF from CTIA - The Wireless Association, Washington, D.C., February 24, 2011

Rosenbluth, Todd, "Standard and Poor's: Industry Surveys, Telecommunications: Wireline," (September 23, 2010): 3. http://www.netadvantage.standardandpoors.com/NASApp/NetAdvantage/showIndustrySurveyPDF.do?loadIndSurFromMenu=pdf.

Shirky, Clay. "The Political Power of Social Media." *Foreign Affairs* (January/February 2011): 35-36.

Sideman, Alysha. "Administration Releases Federal Cloud Strategy". *Government Computer News.* (14, Feb 2011) 1-2. http://gcn.com/articles/2011/02/14/federal-cloud-computing-strategy-released.aspx?p=1.

Standard & Poor's. "Industry Surveys, Computers: Hardware." (October 2010): 18.

Statement of the Press Secretary, August 13, 2009. http://www.whitehouse.gov/the_press_office/Statement-of-the-Press-Secretary/.

"Study: Cybercrime cost firms $1 trillion globally." *CNET News Online* (January 28, 2009). http://news.cnet.com/ 8301-1009_3-10152246-83.html?part=rss&subj=news&tag=2547-1_3-0-20.

"Submarine cable trial lights path to greater capacity for global networks," *Webwire* (March 10, 2011). http://www.webwire.com/ViewPressRel.asp?aId=133656.

Suster, Mark. “Social Networking: The Past.” *Tech Crunch* (December 10, 2010). http://techcrunch.com/2010/12/03/social-networking-past.

Swain, Sampad. “Social Network Monetization – Deeper Insights.” May 26, 2009. http://sampadswain.com/2009/05/social-network-monetization-deeper-insights/#.

Symantec.corp “Virtualization and Cloud Technologies Add Complexity to Disaster Recovery Initiatives.” (2010). www.symantec.com.

Tait, Andrew, and Kurt Richardson. *Complexity and Knowledge Management: Understanding the Role of Knowledge in the Management of Social Networks*. Charlotte, NC: Information Age Publishing, Inc, 2010.

TechAmerica Reacts to President’s Comments on Export Control Reform, March 11, 2010, http://www.techamerica.org/techamerica-reacts-to-president%E2%80%99s-comments-on-export-control-reform.

“Technology and the Advent of Cyberwar.” *Information Security Resources (Online)* (December 15, 2009). http://information-security-resources.com/2009/12/15/technology-and-the-advent-of-cyber-war.

“10 Conservative Principles for Cybersecurity Policy.” *Backgrounder,* The Heritage Foundation (January 31, 2011).

Thormahlen, Casey. “IBIS World Industry Report 51121: Software Publishing in the US.” (February 2011). http://www.ibisworld.com/industryus/default.aspx?indid=1239.

Thormahlen, Casey, “IBISWorld Industry Report 51419a: Internet Service Providers in the US.” (November 2010): 44. http://www.ibisworld.com/industryus/default.aspx?indid=1901.

Thormahlen, Casey “IBISWorld Industry Report 51331a: Voice Over Internet Protocol Providers (VoIP) in the US.” (February 2011): 41. http://www.ibisworld.com/industryus/default.aspx?indid=1901.

Thormahlen, Casey. "Wireless Telecommunications Carriers in the US." IBISWorld Industry Report 51332. www.ibisworld.com/industryus/ default.aspx?indid=1267.

Thormahlen, Casey. “IBISWorld Industry Report 33411b: Computer Monitor & Peripheral Manufacturing in the US.” (February, 2011): 6. http://www.ibisworld.com/industryus/default.aspx?indid=741.

Thormahlen, Casey. “IBISWorld Industry Report 33421: Telecommunication Networking Equipment Manufacturing in the US.” (February 2011): 20. http://www.ibisworld.com/industryus/default.aspx?indid=745.

Thormahlen, Casey. "IBISWorld Industry Report 33411a: Computer Manufacturing in the US." (February 2011): 22. http://www.ibisworld.com/industryus/default.aspx?indid=740.

Thormahlen, Casey. "Internet Publishing and Broadcasting in the US." (February 2011). http://www.ibisworld.com.

Tobin, Jim. "Top 50 Branded Facebook Fan Pages, February 2011." *Ignite Social Media.* http://www.ignitesocialmedia.com/facebook-marketing/.

Traian, Anderei. "Cloud Computing Challenges and Related Security Issues. A Survey Paper". (2009). http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html.

"2010 Africa - Fixed-line Telecommunications and Infrastructure Statistics." Executive Summary. *BuddeComm.* http://www.budde.com.au/Research/2010-Africa-Fixed-line-Telecommunications-and-Infrastructure-Statistics-tables-only.html.

Underwood, Sara. "Social Network Savings." www.myfoxboston.com/dpp/news/special_reports/Social_Network_Savings.

U.S. Department of Commerce, Bureau of Industry and Security, 2004 Policy Controls, "Encryption." http://www.bis.doc.gov/policiesandregulations/04forpolcontrols/chap10_encryption.htm.

U.S. Department of Commerce, Bureau of Industry and Security, "Key Regulatory Areas. http://www.bis.doc.gov/policiesandregulations/index.htm.

U.S. Department of Commerce, Bureau of Industry and Security, "The Wassenaar Arrangement – An Overview. http://www.bis.doc.gov/wassenaar/default.htm

U.S. Department of State, Directorate of Defense Trade Controls, "The Arms Export Control Act." http://pmddtc.state.gov/regulations_laws/aeca.html.

U.S. Department of State, Directorate of Defense Trade Controls, "The International Traffic in Arms Regulation." http://pmddtc.state.gov/regulations_laws/itar.html.

U.S. Department of State, Directorate of Defense Trade Controls, "Commodity Jurisdiction." http://pmddtc.state.gov/commodity_jurisdiction/index.html.

United States Munitions List, found in ITAR, 22 C.F.R. Part 121. http://pmddtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf.

Urquhart, James. "The Biggest Cloud Computing Issue of 2009 is Trust." The Wisdom of Clouds - *CNET News* (2009).http://news.cnet.com/8301-19413_3-10133487-240.html.

VentureDig. "Monetizing Social Networks: The Four Dominant Business Models and How You Should Implement Them in 2010," Venture Dig, November 1, 2009.

Villarreal, Angeles M."CRS Issue Statement on Export Policy," *Congressional Research Service*, January 14, 2010, http://pennyhill.net/documents/export_policy.pdf

Vizard, Michael. "How Cloud Computing Forces the Data Governance Issue. *IT Businessedge* (November 17, 2010). http://itbusinessedge.com/cm/blogs/vizard/how-cloud-computing-forces-the-data-g.

Wassenaar Arrangement, "Control Lists," Category Five, Parts 1 and 2, http://www.wassenaar.org/controllists/index.html.

Waters, Richard. "Technology: A Dip in the Valley." *The Financial Times* (January 19, 2011).

Watkins, S. Craig. *The Young and the Digital: What the Migration to Social-Network Sites, Games, and Anytime, Anywhere Media Means for Our Future*. Boston: Beacon Press, 2009.

Wikipedia, "Cloud Computing Security." http://en.wikipedia.org/wiki/Cloud_computing_security

"Wireless In America." CTIA – The Wireless Association, Wireless In America. http://files.ctia.org/pdf/HowWirelessWorks_jan2011.pdf .

Yang, T., Andrew Yang and Dan Kim. "Social Networking as a New Trend in e-marketing." University of Houston – Clear Lake, TX.

Yasin, Rutrell. "5 Steps to Secure Your Data Center." *Government Computer News* (November 20, 2009): 1-4. http://gcn.com/articles/2009/11/30/5-steps-to-a-secure-data-center.aspx?p=1.

Yasin, Rutrell. "After Data Center Consolidation, Beware Legacy Apps." *Government Computer News* (January 14, 2011): 1-2. http://gcn.com/articles/2011/01/14/afcea-data-center-consolidation.aspx?p=1.

Yasin, Rutrell. "Agencies, Choose Your Clouds-Here Are 3 Basic Options." *Government Computer News* (February 4, 2011): 1-3. http://gcn.com/articles/2011/02/07/Feature-cloud-sourcing.aspx?p=1.

Yasin, Rutrell. "Can Agencies Cut 800 Data Center? Maybe, But Here's What's in the Way." *Government Computer News* (January 6, 2011): 1-2. http://gcn.com/articles/2011/01/06/Data-center-consolidation-OMB-25.aspx?p=1.

Yasin, Rutrell. “Data Center Consolidation a Decade Away, Report Says.” *Government Computer News* (September 23, 2010): 1-2. http://gcn.com/articles/2010/09/23/INPUT-data-center-consolidation-Report.aspx?p=1.

Yasin, Rutrell. “DHS Offers E-mail Services Via Private Cloud.” *Government Computer News* (August 31, 2010): 1-2. http://gcn.com/articles/2010/08/31/Richard-Spires-DHS-Data-Center-Consolidation.aspx?p=1.

Yasin, Rutrell. “Federal Agencies in the Cloud.” *Government Computer News* (February 4, 2011): 1-2. http://gcn.com/articles/2011/02/07/Feature-Cloud-Sourcing-agency-list.aspx?p=1.

Yasin, Rutrell. “Implementing the Cloud-First Policy? Start with E-mail.” *Government Computer News* (December 17, 2010): 1-2. http://gcn.com/articles/2010/12/17/Cloud-First-Policy.aspx?p=1.

Yasin, Rutrell. “State IT Diet: Consolidation, Cloud, and Shared Services.” *Government Computer News* (February 4, 2011): 1-2. http://gcn.com/articles/2011/02/07/Federal-Cloud-Sourcing-Side-1.aspx?p=1.

Yasin, Rutrell. “The Political Hurdle to Data Center Consolidation.” *Government Computer News* (June 8, 2010): 1-2. http://gcn.com/articles/2010/06/08/data-center-consolidation.aspx?p=1.

Yasin, Rutrell. “What’s Ahead for Government IT in 2011?” *Government Computer News* (January 19, 2011): 1-2. http://gcn.com/articles/2011/01/19/IDC-government-insights-2011-predictions.aspx?p=1.

.

..

.

.