Spring 2008
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 2008

ABSTRACT: The Information and Communications Technology (ICT) industry is vital to the United States' national security and our economic strength, and has been the catalyst for the economic boom observed in the world over the past ten years. Because of its strategic importance, the ICAF has commissioned the ICT industry study group to examine the economic, strategic, and technological strengths and weaknesses of the domestic and international companies that make up this industry. The Group synthesized the knowledge to formulate a comprehensive view of the ICT industry and formed recommendations for government's role in facilitating ICT industry growth and development.

Lt Col Timothy Applegate, US Air Force
Lt Col Ronald Baldinger, US Air Force
LTC Martin Bremer, US Army
COL Robert Claflin, PhD., US Army
COL Mohammed Gadih, Moroccan Air Force
COL Brian Haebig, US Army
CDR Thomas Kollie, US Navy
Mr. Todd Kushner, Department of State
CAPT James Kuzma, US Navy
Mr. Brian Landers, Department of the Navy
Ms. Jennifer Lasichak, Department of the Army
COL Warren O'Donell, US Army
Lt Col Kenneth Plaks, PhD., US Air Force
Mr. Todd Ramsey, Raytheon Corporation
CDR Charles Sellers, US Navy
CDR Charles Taylor, US Navy
LTC Julian Williams, US Army
Lt Col Bryan Witeof, Air National Guard

COL Richard Altieri, US Army (Retired), Faculty
Col David King, Canadian Forces (Retired), Faculty
Col Lynne Thompson, PhD., US Air Force (Retired), Faculty
CDR Feza Koprucu, Department of Homeland Security Chair, US Navy (Retired) Faculty

PLACES VISITED:

Local Visits and Speakers:

IBM Federal Systems, Washington D.C.
Comcast Cable Corporation, Washington, D.C.
CTIA, The Wireless Association, Washington D.C.
Cyber Trust, ICSA Labs, a division of Verizon, Inc., Mechanicsburg, PA
Information Technology Association of America, Rosslyn, VA
The Information Technology and Innovation Foundation, Washington, D.C.
National Cable and Telecommunications Association (NCTA), Washington, D.C.
National Telecommunications & Information Association (NTIA), Washington, D.C.
Northrop-Grumman, Northrop Grumman Information Technology, Reston, VA
Nortel Government Solutions, a division of Nortel Networks Ltd, Fairfax, VA
Novak Biddle, Venture Partners, Bethesda, MD
Software & Information Industry Association (SIIA), Washington D.C.
Sprint-Nextel, Reston, VA
Telecommunications Industry Association, Washington D.C.
The John Kneuer Company, LLC, Washington, D.C.
Verizon Communications, Washington, D.C.
Vonage Holdings Corporation, Washington, D.C.

Domestic:

Brocade Communications, San Jose, CA
Cisco Systems, San Jose, CA
Foundry Networks, Santa Clara, CA
Google, Mountain View, CA
Juniper Networks, Mountain View, CA
National Semiconductor, San Jose, CA
Oracle, Redwood Shores, CA
Sun Microsystems, Santa Clara, CA

International:

American Chamber of Commerce, Taipei, TW
American Institute in Taiwan (AIT), Taipei, TW
BDA China, Beijing, PRC
BenQ Corporation, Taipei, TW
Chinese Academy of Telecom Research, Beijing, PRC
Huyi Tech. Co. Ltd., Guangzhou, PRC
Guangdong Communications Administration, Guangzhou, PR
China Internet Network Information Ctr., Beijing, PRC
Chunghwa Telecom, Taipei, TW
Digital United (SeedNet), Taipei, TW
Google China, Beijing, PRC

INTRODUCTION:

The Information and Communications Technology (ICT) industry is critical to the prosperity and security of the United States of America. First, ICT and its applications continue to drive U.S. productivity and economic growth. The ICT revolution is a large and persistent positive supply shock, facilitating higher, more stable economic growth and inflation mitigating productivity growth. Second, ICT provides the infrastructure and capabilities that form the basis for the command, control, and communications systems that underlie U.S. national security. The U.S. faces challenges in maintaining ICT derived economic strength and command and control in the advent of a cyber attack, terrorist attack, natural disaster or other disruptive incident that could damage the nation and potentially threaten national sovereignty. Therefore, the United States must set conditions that secure the nation's ICT infrastructure.

Furthermore, ICT innovation and application are inextricably linked to global economic relevance and leadership. The industry continues to benefit from the financial mediation of venture capital investment in entrepreneurial ICT businesses, which drives America's ability to maintain this momentum of innovation. Innovation will continue to drive the development and application of information and communications technologies, which will improve business performance by increasing productivity.

The ICT industry is a dynamic industry that in many respects is still in its infancy. Software as a Service (SaaS) and cloud computing will continue to emerge as bandwidth increases, data security improves, and assured access reaches new users and quickens the pace of globalization. Market motivated infrastructure investment in broadband, to include the fiber optic backbone and third and fourth generation (3G & 4G) wireless technologies, will create a robust mobile experience, broadening and deepening the impact of ICT-enabled transactional processes. Mobile capabilities will match fixed capabilities. Productivity will realize an order of magnitude increase, as economic output becomes increasingly a function of this mobile, continuously connected collaborative-networked world.

Public policy will continue to play a significant role in the industry. Decisions made by legislators and regulators on key ICT market mediating policy issues such as net neutrality and R&D incentives will impact markets, as will decisions made in international bodies regarding technical standards, anti-trust, and critical information infrastructure protection (CIIP) issues. To ensure U.S. competitiveness, the government must remain wary of technology trade barriers and populist sentiment for debilitating autarkic regulation.

Internationally, Taiwan and China's ICT industry was studied as a point of comparison to better understand the industry's international impact. The ICT industry in both China and Taiwan has experienced robust growth with positive effects on their economies. However, both suffer from growth constraining de facto regional monopoly market structures similar to that of the U.S. several years ago with the regional Bell operating companies (RBOCs). Furthermore, both predominantly employ copper-based ADSL technology for delivery of broadband services, a constraint on future broadband and market growth.

This paper will compare the US ICT industry to the international ICT industry as it considers the timely and relevant issues that are critical to the industry's continued contributions to the U.S. and the world's economic welfare. In sum, this paper will provide the reader a broad appreciation of the ICT industry, the related policy issues, and how ICT can continue to be a driving force of U.S. national power.

THE INDUSTRY DEFINED:

The ICT sector has been officially defined by the Organization for Economic Co-operation and Development (OECD) countries as "the combination of manufacturing and services industries that capture, transmit, and display information electronically" (OECD 2002, 19). This definition encompasses a wide range of industries and markets including electronics and components, information technology (IT) equipment and systems, communications equipment and systems, IT services, software, telecommunications and cable services. Increasingly, digital content and the digital content providers are important drivers of the ICT industry (OECD 2006, 34-81).

CURRENT CONDITION:

In an increasingly interconnected world, today's decisions and actions travel through space and time using ICT. Indeed, no other industry touches as many technology-related business sectors as telecommunication, which, by definition, encompasses not only the traditional areas of local and long-distance telephone services, but also advanced technology-based services including wireless communications, the Internet, fiber-optics and satellites. The ICT industry is advancing economic welfare everywhere and evolving the world's economies. Rapid innovations in Internet and wireless technologies are driving this advancement, quickly changing consumer preferences and disrupting traditional communication methods.

Two-thirds of ICT generated U.S. GDP comes from ICT used in non-ICT industries (Martikainen 2007). The U.S. Department of Commerce asserts that the United States maintains global information and communication technology leadership and economic strength. The National Telecommunications and Information Agency (NTIA) points to the sustained growth of the U.S. economy and a $13.2 trillion gross domestic product, unemployment below 4.4%, growing e-Commerce revenues of $60 billion in 2004, and over $400 billion in information technology investment in 2005. "The information and communication technologies sector is the fastest growing part of the United States' economy" (Drennan 2002). The ICT sector employs 2.7 million Americans, a 17 percent net growth between 1997 and 2006 (SIIA 2008). As a result of this investment, approximately 11% of the growth in GDP is directly attributable to ICT for 2004 and 2005, a growth rate that is three times higher than the U.S. economic growth overall.

Mergers, acquisitions, and other industry changes continue to shape the market. An oligopoly of large telecommunication and cable companies are competing fiercely with each other using differing technologies, including broadband Internet, video, telephone, and mobile service that characterize the current U.S. market. AT&T and SBC merged (AT&T, Inc.), and Verizon absorbed MCI. Sprint and Nextel united to create Sprint Nextel. The competitive backdrop is changing radically due to these mergers. Verizon and AT&T Inc., two of the seven firms that were created from the pieces of the old national telephone monopoly (AT&T – broken up by the courts in 1984 for anti-trust reasons) dominate the bevy of companies that evolved mainly from the wireline and wireless telephone voice networks (Rosenbluth 2008, 8-9; Rosenbluth 2007, 2). However, the advent of broadband Internet has resulted in the large cable companies — Comcast, TimeWarner, Cox Communications Inc., and Charter Communications Inc. — entering into Verizon/AT&T markets. These markets now account for nearly 75% of the cable industry's subscriber base and 80% of cable's $75 billion in annual revenues (Amobi 2007,

7). As of September 2007, cable firms accounted for 54% of broadband connections, while digital subscriber line (DSL) comprised 46% (Rosenbluth 2007, 5).

Wireless access to the Internet also threatens traditional cable broadband suppliers. Municipal Wi-Fi systems are being developed offering citywide, high speed, wireless Internet connections at no cost or at prices much lower than DSL or cable access. However, Wi-Fi communication is limited to a range of roughly 150 feet. WiMax, an advanced wireless technology with a range of up to 30 miles, has the potential to be a disruptive technology and impact traditional broadband, cell phone, landline, and Wi-Fi systems further increasing competition.

Nevertheless, the frequency spectrum available to accommodate these new technologies and business plans is limited with demand being greater than available spectrum. The global transition to digital television is currently the most promising opportunity for spectrum reallocation, by making use of gains in spectral efficiency provided by conversion from analog signals. There are three broad categories of stakeholders in spectrum management: the ICT industry, governments, and citizens, each with their own particular interests. Industry seeks access to additional spectrum at the lowest possible cost, while minimizing potential uncertainty associated with government regulations. Additionally, firms benefit from standardization of frequency assignments and modulation methods across jurisdictions. Firms are also concerned with promoting wireless spectrum regulations that support their business models.

At the same time, Verizon and AT&T are laying fiber-optic cable directly to neighborhoods, homes, and offices in pursuit of customers with promises of ultra-high-speed Internet connections and enhanced content. Verizon believes so strongly in the potential for broadband deployment to be an engine of growth that it has adopted a “bet the company” strategy — fiber to individual homes/businesses — aiming for 89 million households to have fiber optic Internet by 2010. AT&T Inc. is the largest player in the U.S. market, with 17 million DSLs and 17% ISP market share as of the first quarter of 2007. Comcast is next with 12.1 million cable broadband subscribers and 12.1% share for the same period. AOL fell to third place, with 11.9 million broadband subscribers and 12% share. The top six ISPs control 61.1% of the market (Rosenbluth 2008, 5).

Companies realize customers do more than just watch television, surf the Internet, and talk on the phone. The reality is that most people use several services and that has left most service providers trying to find ways to attract those customers. Some companies are offering bundled service packages (combining wireless accounts, high-speed Internet access, entertainment such as video on demand and TV via IP, in addition to Voice over Internet Protocol (VoIP) or landlines) available for a lower cost than purchasing them individually. These bundles are a marketing tool, but it appears broadband is where all companies see the opportunities for further growth.

In the U.S., cellular phone companies are upgrading and expanding their 3G networks. The upgrade will enhance service with 3G features such as multimedia, Internet access, and video footage that consumers in other countries already enjoy. In addition, government regulations are evolving quickly, bringing even bigger changes to business strategies. Overall, the telecommunications industry is in a state of continuous technological and economic flux driven by intense competition and new technologies that benefit consumers.

The growth of computer commercial services (CCS) is one of the many outcomes of the ICT expansion. This industry enables businesses to save money by using outside computer specialists for many of the computer related tasks previously performed in-house. The CCS

industry has two segments: professional service and business processing. There are ten large firms, e.g., IBM, EDS, Accenture, which account for 25% of the professional services segment. In contrast, business-processing services has a small number of dominant players catering to each segment of the processing market. U.S. firms that offer CCS have turned to international offshoring to supply many of their activities – one estimate predicts that from 2006-2011, offshore ICT spending will increase 16% annually to top $28 billion (Cathers 2007, 3,6,12, 16).

Notwithstanding its past performance and future promise, as the ICT industry expands globally, qualified human capital may become a constraint. According to the Bureau of Labor Statistics, demand for network systems and data communications professionals will increase by 53.4% from 2006 to 2016 (Perelman 2007). However, a variety of sources suggest that United States will not be able to meet this demand as U.S. education statistics reflect a serious decline in the number of Science, Technology, Engineering, and Mathematics (STEM) graduates; i.e., the number of "home grown" STEM graduates has declined. Conversely, science-based graduates have increased dramatically in India and China, among other countries. Accordingly, U.S. employers have attempted to import qualified personnel from various countries, but annual non-immigrant visas for skilled workers (H-1B visas) are limited. Companies are now offshoring many of their ICT functions to satisfy their requirements and U.S. statistics still reflect a serious decline in the number of STEM graduates in the U.S.

Even with the human capital shortfalls, the ICT sector's contribution to America's economy continues to grow in magnitude and importance, both directly and indirectly. ICT products, services, and their application are the driving force behind the United States' broader, non-sector specific economic growth of the past decade. U.S. global competitiveness in transactional business is hallmarked by U.S. innovation and the rapid and evolutionary application of information and communication technologies to improve business processes. ICT has created a new global "information economy" where business models are driven by expertise and intellectual capabilities based upon networking, connecting and collaborating (SIIA 2008). Interestingly, ninety percent of information technology employment is outside of the ICT sector. These sectors include agriculture, banking, retail, and manufacturing, where embedded ICT functionality provides increased efficiency and productivity (Tasker and Hodgkins 2008).

Globally, there is no force more notable than the emerging Chinese Internet community. China's government has made development of ubiquitous Internet connectivity to the entire population a 'command' priority. China's Internet connectivity consists of a fiber optic backbone and the combination of hardwired ADSL and 3G wireless for terminal connectivity. China is investing substantially in ICT infrastructure as the government attempts to guess the population's demand for speed and service will be as they become more active on the network. According to the CNNIC (China Internet Network Information Center) Statistical Survey report on the Internet Development in China, China currently ranks second only to the United States in the total number of Internet users, and with an annual growth of 53% per year, will overtake the United States as the largest Internet user community in 2008.

CHALLENGES:

As noted, the ICT industry creates prosperity both in the industry itself; as well in every other industry. ICT is now so pervasive that it is almost impossible to imagine life and an economy without it. The industry has been wildly successful at delivering innovation and revolutionizing both the overall economy as well as government's interaction with its citizens.

Yet, underpinning that success is a sustainability and reliability challenge because of the fragility of the current ICT industry and network. It is fragile on two counts. First, the network and the data that traverse it are not as secure as they need to be. Second, from a personnel perspective, the intellectual capital that brought the U.S. to the forefront of the ICT industry requires replenishment and growth. As the ICT industry grows ever more important to the national economy and well-being, government and industry need to be mindful of these potential weak links to ensure the promise of a globalized, wired, and totally connected nation and world.

INFORMATION SECURITY

The first challenge, ensuring security of the network and its data, is a multi-faceted problem that involves aspects of network security, Critical Information Infrastructure Protection (CIIP) and online privacy. Much is made of the computer industry's birth in hobbyists' garages and college dorms from California to Massachusetts. This grassroots heritage created a mighty industry, but it also created a culture, which that values innovation and performance far more than security. While the hobbyist mentality was fine in its infancy, ICT now commands and enables a significant fraction of the U.S. economy. Security is perhaps now more important than marginally improved performance.

Currently, individual users are responsible for securing the computers, routers, and software that glues the network together. The problem is that individuals tend to under purchase ICT security needs or are ignorant about network vulnerabilities. Some vendors provide security services; but more frequently these are an additional option available for purchase, not an embedded part of the system. However, a network is only as secure as its weakest link and network security is an unfunded economic externality. The challenge is to fund the externality without stifling innovation and network growth. One approach would be to regulate that ICT vendors are liable for security just as automakers are liable for automobile safety. By shifting the burden of responsibility from individual consumers to network producers, this may solve the externality and vastly improve network security, albeit at an added cost to consumers.

Non-secure networks also pose a challenge to the critical infrastructure that undergirds modern society. The network controls international banking, traffic signals, water and oil pipelines, electrical grids, etc. These networks are vulnerable to malicious intrusion. Since 90% of U.S. critical infrastructure is in private hands, the Department of Homeland Security must work with industry to ensure that the industry's security investment calculations go beyond individual firm's economic efficiency and provide for the public good. Globally, malicious intrusion needs to be mitigated by international cooperative security agreements to synchronize global protection, planning and law enforcement against cyber-crime and deliberate disruption. This implies interagency cooperation between the State, Homeland Security, Justice and Commerce Department as a necessary precondition for progress.

Another challenge lies in determining the correct balance between the benefits of the interconnected world and threats to privacy from those same technologies. Many users expect privacy online, yet the collection and monitoring of personal information for both honorable and some not so honorable intentions frequently occurs. Though the industry has attempted self-regulation, their efforts are focused on economic performance and not necessarily the privacy interests of the consumer. Where legislation exists, it is often ad-hoc and inconsistent. The government's challenge is to educate the public on their rights and incentivize notification and privacy protection principles nationwide and ideally, internationally.

MAINTAINING U.S. COMPETITIVENESS

The second challenge is replenishing the ICT workforce and preserving and enhancing the public policies that have led to U.S. industry's success. The industry was largely "born" in the U.S. due to its excellent universities and entrepreneurial spirit. However, the knowledge-based ICT industry, mobile by its very nature, is free to leave should the U.S. under invest or adopt counterproductive policies. Therefore, the U.S. needs to preserve and enhance the factors that created the industry in addressing the challenges that face the industry.

Human capital is the resource that enables the knowledge-based economy. Between the baby boom and the space-race, the U.S. enjoyed a healthy supply of highly trained, highly motivated people to create the ICT industry. However, demographics are shifting and the U.S. must shift as well to deal with the new reality. First, fewer Americans are studying a STEM curriculum. The government could do much to incentivize STEM studies through targeted subsidies, such as National Science Foundation scholarships and student loan forgiveness for STEM graduates. Second, even if there were no percentage change in the number of STEM students, with the impending retirement of the baby-boomers, there will be a shrinking population of workers to replenish a growing industry. Therefore, America needs to remain true to its history and embrace highly skilled immigrants. By increasing and easing immigration for ICT workers, the U.S. can remain the engine of ICT growth. Embracing and offering citizenship to other nations' best and brightest has always served America's self-interest; excluding them does not and incurs lost opportunity cost.

The U.S. has led the world in ICT innovation. Now the U.S. must innovate not just in technology, but also in its public policy. The U.S. should lead the world in addressing the myriad of information security, CIIP, and privacy challenges created by the new technology. By recognizing the public good aspect of network security, the U.S. can facilitate the continuation of a vibrant industry. The U.S. must also rise to the challenge of a globalizing, post-industrial world by supporting STEM studies and simultaneously embracing immigration. The ICT industry's potential is limitless, but is dependent upon American society's willingness to nurture it.

OUTLOOK:

Driven by innovation, entrepreneurial spirit, and increasingly freer flow of information, the ICT industry transformed global commerce, culture, and governance in a phenomenon characterized as the "Information Revolution." This explosion of communication and unfettered information, with its speed and pervasiveness, has unprecedented worldwide reach. This has empowered individuals, business and nations with new means of exercising the informational component of national power formerly reserved to and constrained by governments. The information revolution has resulted in a profusion of new technologies, applications and methods of exchanging information and freedom to enjoy economic and social betterment.

Rapid changes in the communications landscape resulting from technological changes and the development of new services, platforms and greater capacity are transforming the industry along numerous vectors, changing almost every aspect private and public life. A 2006 Rand study concludes that the "…the rate of growth of computational speed, memory density, reduction in the cost per computation or other performance specifications through 2020 is highly feasible." (Rand 2006, 4) Providing that this trend of increasing computing and networking power continues, the ICT market will continue to expand domestically and internationally.

Within the next five years, Software as a Service (SaaS) will expand to provide over 25% of all business applications (Khahil 2006, 1). Cloud computing, also known as grid computing, means centralizing data and computing power in secure locations. It delivers data services to end users interacting on simplified display terminals known as thin clients. SaaS and cloud computing, enabled by the growth of high-speed networks, will continue to grow in market share due to the inherent economies of scale provided by centralization. Cloud computing can eliminate the need for organizations to centrally manage software and data storage, and can reduce the need for powerful desktop computers. Google, Sun and other major cloud computing providers will reduce the need to stay near a workstation or carry a pocketful of thumb drives. SaaS and cloud computing can provide users with on-demand ability to access and manipulate the information they require, from any location, using just a web browser (Cord 2008). Network security requirements will increase in importance. Authentication methods such as biometrics or even micro-chipped individuals, similar to those used on pets today, will become commonplace.

While ICT firms remain concerned about their ability to hire the best and brightest engineering graduates from prestigious universities in the U.S., wage growth has been insufficient to entice American students into that field of study. Foreign students comprise a significant portion of engineering students in leading universities (Conyers 2007, 9). Recruiting and retaining foreign students as employees has been a challenge for U.S. firms because of highly restrictive immigration regulations. As one example of industry response to U.S. immigration policy, Microsoft built a new research facility in Vancouver, Canada (Broache 2008, 1).

The ICT industry revolves around innovation and the marketing of new products. Significant growth opportunities remain through improving efficiency via diverse applications such as electronic health care records, geolocation-aware services, and cloud computing. With the advent of nanotechnology and highly durable processors, products on the drawing board today will be commonplace in 2020. Computers will find their way into an increasing number of applications, such as wearable computers for communications and medical sensing.

The future of the ICT industry is mobility. Consumer demand for wireless broadband services will grow exponentially and lead a corresponding increase in radio spectrum use. The current markets of telephone, cable, and wireless providers overbuilding each other's networks while competing with individuals and firms operating wireless networks in homes and offices will enhance broadband service competition. ICT firms will build new high-speed wireless networks employing 4G technologies such as Long Term Evolution (LTE), Ultra Mobile Broadband (UMB), and WiMax. However, technological developments may not be sufficient to meet growing spectrum demand because they require the use of progressively higher frequencies than in the past. Today's spectrum frontier lies in the millimeter-wave band between 30 and 300 GHz, but semiconductor technology will not enable high data rates there for 5 to 10 years. (Ravazi 2008) Millimeter waves have very short ranges and are poorly suited for mobile service to roaming users. Therefore, additional mobile bandwidth must come from market pressure for new models of spectrum management or reallocation.

The current state of worldwide frequency band assignments reflects a combination of International Telecommunications Union (ITU) agreements and various national government laws and regulations enacted over the past century when telecommunications was regarded as a natural monopoly. In the U.S., radio spectrum is a public resource apportioned by the FCC for the public good. Regulation of wireless airwaves has grown into a patchwork of users distributed haphazardly throughout the spectrum. This model of carving out defined portions of

the spectrum for unique allocation is increasingly inefficient, particularly in light of growing demand and market and industry expansion. Software-defined radio (SDR) technology enables another model. SDRs, via cognitive radio or dynamic frequency assignment capabilities, can react to interference and competing signals by automatically moving to an empty frequency in milliseconds.

The last decade has seen a formidable increase in ICT industry capabilities and capacity, ranging from connectivity to microelectronics to services. The world is merging into an information grid that becomes more redundant and intertwined every day. Moore's Law will remain valid as the ICT industry continues to thrive, evolve, and enmesh every facet of daily life.

GOVERNMENT GOALS AND ROLE:

Governments have historically played significant roles in regulating telecommunications providers and the shared commons of the radio frequency spectrum thereby balancing the benefits to individuals, firms, and society. Two potential approaches exist and the U.S. government is attempting to balance between them. The first approach is to establish domestic and international laws and regulations to govern the shared commons that is today's global network. Governments have intervened in issues such as email transmission, phone calls, electronic banking transactions, and data retention requirements. Governments may have a further role to play in other domestic and international challenges such as privacy protection, intellectual property, and market concentration issues.

Alternatively, governments may choose to take little or no action, allowing the market to determine the best course for the industry. Counter to observations made in Taiwan and China, and noted in numerous other countries, the U.S. ICT industry is shaped less by government and more by technological and financial decisions made by ICT firms and consumers, i.e., markets. Software code, hardware capability, and networking protocols are often limiting factors and more influential than laws and regulations in dictating the course of the industry. The optimal synthesis of these two approaches is to limit government regulation to those functions that are inherently governmental, such as common security or as a corrective action in the presence of a market failure.

For example, it is probably inadvisable for governments to enact network neutrality rules. While proposals vary, most approaches represent a form of rent seeking by the content industry and would represent a return to the limitations inherent in the legislated common carrier era. Carriers have both the right and obligation to manage their networks in order to prioritize data streams such as voice, video, images, and text as determined by the consumers they serve. Increased competition from fiber and wireless networks overbuilding cable and DSL will obviate the need for government to regulate the flow of content. Due to the rapid pace of technology change, attempts at network neutrality regulation would soon become irrelevant and perhaps even counterproductive. Instead, the government should adopt policies designed to improve competition and increase end-user choices, just as it did with the breakup of the Bell System.

The President's 2003 Spectrum Policy Initiative began to explore the feasibility of new models of spectrum allocation. SDRs can enable spectrum sharing agreements between wireless providers and potentially compatible services such as broadcasters, government services, public safety, and the military. However, this policy initiative experienced significant delays in achieving consensus between government and industry. Congress is investigating why the "D block" of 700 MHz spectrum failed to reach its reserve price in the FCC's 2008 auction. One

potential cause was industry concern over the impact of requirements to share this block between telecommunications providers and public safety services. Thus, the benefits of SDRs are more likely to come from market-driven agreements that promote efficiency via real-time spectrum trading. Another alternative model of spectrum allocation is to set aside so-called "white spaces" for unlicensed devices such as cordless telephones or Wi-Fi computer networks, which mitigate interference through dynamic frequency assignment. Individuals and firms seeking inexpensive, local access to spectrum are likely to favor expanded use of white spaces. Incumbent licensees and those with significant investments in the status quo are likely to oppose this approach.

Enacting property rights via licensing promotes market competition and efficiency. However, licensing fees for broadcasting and telecommunications differ significantly. Annual fees for television stations to use 6 MHz of spectrum range from $64K in the top 10 markets, down to $5K in smaller markets. In contrast, the FCC raised $19.6B from auctioning ten-year licenses on 62 MHz of former 700 MHz TV spectrum to wireless providers. (FCC 2008)

The FCC should allocate additional telecommunications spectrum to reflect its market value. One such proposal came from Google's March 2008 public filing with the FCC, proposing to free up spectrum by changing the model for protecting television stations from interference. Instead of geographic and frequency separation between channels, this plan would reallocate these buffers as white spaces for low-power unlicensed devices, with Google databases and SDRs preventing interference. However, the FCC should not outsource its responsibilities to protect licensees from interference. Instead, the FCC could mandate reuse of digital television channels at shorter geographic separations, and subsequently reallocating a band of freed spectrum for telecommunications. This would entail moderate reductions in television coverage areas, which would go largely unnoticed due to increasing consumer reliance on cable, fiber, and satellite for television and other services. The FCC could then auction some of the reclaimed spectrum, reserving the remainder for competing low-power unlicensed devices.

How can governments influence broadband leadership? Governments in China and Taiwan have adopted the approach of regional monopolies backed by state investment and ownership and regulated tariffs that discourages improved infrastructure development. The net result is that while the Chinese ICT industry has impressive penetration, affordability, and accessibility statistics, it offers limited performance. Their approach to technological convergence is telephone-based. Government regulations inhibit cable companies from competing to deliver Internet service. The vast majority of wired services are copper-based DSL, with downlink speeds limited to two Mbps. China is preparing to roll out its 3G mobile network, while U.S. firms are now preparing to deploy 4G networks. Since Chinese companies face no competition and are constrained by low subscriptions fees, there is minimal incentive for firms to upgrade their networks and offer improved services. Rather than take this common-carrier era approach, the U.S. should continue its policies of relaxing overt telecommunications regulation, opting instead for incentive-based approaches that promote competition, private ownership, and market forces. Free markets remain the best path to broadband leadership and improved consumer benefit.

The lack of coordinated communications and equipment interoperability between local, state, and federal government organizations on scene during emergencies have often hindered responders' efforts. Non-interoperability has led to lack of timely notification of developing hazards, contributed to coordination failures in public service emergencies and unnecessary endangerment of public safety personnel. Although there have been many opportunities to garner lessons learned and correct communications interoperability issues, governments and

industry have yet to solve this public goods problem. Obstacles have included physical limitations of the equipment used by public safety organizations, such as incompatible frequency bands and limited procurement funding. Leadership challenges include incompatible management structures, institutional controls, and cultures (Smith, B., Tolman, T. 2000, 17).

Since industry is developing technology that has the potential to overcome the lack of interoperability, the federal government's focus should be on defining technology standards to ensure interoperability. The Department of Homeland Security's April 2004 SAFECOM Statement of Requirements for public safety communications interoperability is the foundation for these standards. This work, in partnership with the Project 25 effort within the private sector, could potentially solve the interoperability problem. Therefore, the federal government should regulate that local, state, and federal public safety organizations purchase Project 25 compliant communications equipment. This will take time due to the large capital expenditures required, but if these organizations achieve compliance, the lack of interoperability can be resolved.

While the U.S. ICT industry remains healthy, the issues discussed above potentially threaten its future promise. To maintain a growing economy while ensuring an effective homeland defense, the federal government needs to assiduously examine the challenges and adopt the appropriate policies. Government should employ regulation as a means of problem solving as a last resort, limiting itself to inherently governmental issues or where market forces have produced glaring externalities and proven ineffective.

ESSAYS ON MAJOR ISSUES:

The following essays provide a synopsis of the major issues facing the U.S. ICT industry and how these issues potentially affect U.S. economic performance and national security.

ICT CAPACITY IN A NATIONAL SECURITY EMERGENCY

The Department of Homeland Security (DHS) defines *interoperability* as "the ability of emergency response agencies to talk to one another via radio communication systems – to exchange voice and/or data with one another on demand, in real time, when needed and when authorized" (U.S. Department of Homeland Security 2008, 1). Two major efforts have commenced within the federal government to overcome the issue of communications interoperability between local, state, and federal public safety organizations. The first is the creation of the SAFECOM program within DHS, which provides research, development, testing and evaluation, guidance, tools, and templates on communication-related issues to local, tribal, state, and federal emergency response agencies (U.S. Department of Homeland Security 2008, 1). The release of SAFECOM's Statement of Requirements for public safety communications interoperability in April 2004 has been significant. This initiative provides future requirements for crucial voice and data communications in day-to-day, task force, and mutual aid operations (U.S. Department of Homeland Security, 2008 p.1). SAFECOM's effectiveness in overcoming the interoperability problem, however, has been less than optimal (Government Accountability Office, 2007, p. 3).

The second effort commenced by the federal government has been the creation of the National Response Plan (NRP), as required by Homeland Security Presidential Directive (HSPD)-5 (U.S. Department of Homeland Security 2004, 1). The second of 15 Emergency Support Functions (ESF) within the NRP focuses on communications. The scope of ESF #2 is to provide required temporary National Security and Emergency Preparedness (NS/EP)

telecommunications and the restoration of the telecommunications infrastructure. It also supports all federal agencies in the procurement and coordination of NS/EP telecommunications and information technology (IT) requirements during an incident response to provide communications services.

Within the private sector, actions have also been taken to overcome the lack of interoperability amongst public safety organizations. Some of the advancements being developed by private industry include technology that bridges communications gaps between disparate legacy systems, new technologies that are inherently interoperable to replace the legacy systems, and mobile systems that can be rapidly deployed in a national security emergency to temporarily replace damaged communications infrastructure or to provide additional communications capabilities. Unfortunately, the lack of standards concerning public safety communications technology has hampered this development of interoperable equipment.

In an effort to create standards that would allow manufacturers to develop and make interoperable communications equipment, a committee of manufacturers, public safety agencies, and state and federal communications organizations was formed. This committee became known as Project 25. Since 1989, completion of four of the eight interface subsets has occurred with three of the four completed during the 2005 – 2007 period (Government Accountability Office 2007, 41). Overall, the GAO has identified four obstacles to communications interoperability: standards are incomplete or not well defined, lack of compliance testing has limited product interoperability, state and local agencies do not know how to select Project 25 products, and complete Project 25 systems can be prohibitively expensive (Government Accountability Office 2007, 36 - 38).

The market for interoperable public safety communications is extremely fierce with many companies competing to provide their solution to the problem. In addition to the myriad of infrastructure compatibility solutions, many telecommunications companies have developed rapid response capabilities to temporarily restore connectivity when the infrastructure is unavailable or extra capacity is required. Some examples include Rivada Network's ICES system, Verizon's Disaster Response Teams, Sprint's Emergency Response Teams, and AGTFederal's Mobile Incident Site Systems.

Recommendations for positive gain in ICT capacity in a national security emergency are: (1) the federal government must continue to define and regulate the standards for public safety communications technology; (2) the private sector must continue to develop near-term solutions by building technological bridges between legacy communications systems; and (3) as 4G wireless technologies continue to develop and become available, the federal government must support public safety organizations at the local, state, and federal levels with grants to upgrade their communications systems as required to meet this public goods requirement.

Ultimately, it will take all of the above recommendations together with time and a continued dialogue between all levels of government and private industry to arrive at a solution that will allow public safety organizations at all levels to communicate seamlessly during a national emergency. (CDR Sellers)

ICT INFRASTRUCTURE PROTECTION

Information power has dramatically altered the world to the point that a new global information economy has formed that blurs both geographic and geopolitical boundaries (Gansler 2004, 15). However, international doctrine and law have not kept pace with the changing economic practices of the global information economy (Arquilla and Rondelft 1999,

57). For example, the lessons learned in the Estonia cyber-attacks showed that there were no international laws in place to respond to the attacks and no governance structure to guide reaction to an incident (Bright 2007). Addressing this lack of governance is time critical because as global interconnectivity increases, so does the number of cyber-attacks (Cashell 2004, 1). Therefore, it is in the national interest to formulate international collective security agreements that address this lack of governance. According to a study on information strategy by the RAND Corporation:

> *From an economic-legal perspective, this cooperation may depend upon reaching agreement in several issue areas, beginning with what might be called "substantive law." This notion basically calls for agreement as to what constitutes a "crime," including fraud, forgery, hacking, and sabotage (or, as we have called it, "cybotage"). …In the information realm, agreement about such matters as territoriality, extradition, and the notion of "hot pursuit" may form a minimum basis for international cooperation. The challenge will be to harmonize these bases for cooperation—especially in the area of cyberspace-based territoriality—with the noosphere (Arquilla and Rondelft 1999, 57).*

Truly, the collaborative dialogue necessary to establish these international security agreements on cyber-attacks, cyber-crime and other cyber-economic issues will require a joint inter-agency action by America's diplomatic, legislative, and judicial systems. Close coordination by the departments of State, Homeland Security (DHS), and Justice is required to ensure international CIIP agreements encompass prospective threats and are responsive enough to adapt to the changes in technology. Additionally, private sector involvement is critical to any effective CIIP policy formulation due to private ownership of 90% of ICT critical infrastructure (Juster 2002, 4). Government and private sector cooperation will facilitate the ability to stay abreast with technology changes and will provide another venue, via interested stakeholders, to monitor and adjust policies and procedures to the changing threats to ICT infrastructure.

Long-term collective security agreements afford the opportunity to impede transnational cyber-crime and cyber-attacks and benefit all partnered national economies in an area where market forces do not supply sufficient impetus or profit to provide protection. Moreover, these cooperative agreements become more valuable to the international system and the United States as the amount of international trade of goods, intellectual property, on-line transactions, and globalization increases. In sum, CIIP collective security agreements will reduce risk to all national economies, are necessary to provide governance in the information age, and require immediate implementation. (CDR Kollie)

INTERNET AND NETWORK SECURITY

The Internet is a key enabler of national power, yet the network is fragile and vulnerable to disruption. Internet security is a public good and as such, is underpurchased by individual users. For instance, to be reasonably secure, a computer requires updated virus and spyware protection as well as a secure firewall; yet a recent study found that 81% of home computers lack at least one of these. (AOL/NCSA 2005) Accordingly, it may be appropriate for the federal government to act. Instead of continuing to treat computers as if they were independent nodes that do not affect each other, the federal government should adopt a public good paradigm. By requiring manufacturers to sell secure products and keep them secure, it can make the would-be

computer criminal's task much more difficult. By further co-opting Internet service providers (ISPs) to enforce these standards the government can keep the network far more secure while avoiding stifling excesses.

Historically, Internet regulation arose out of the telecommunications industry, and most existing regulation concerns access or content, not security. The federal government should mandate that all computers sold in the U.S. meet certain basic security standards. These standards would be developed by a collaborative partnership between the government, industry and security experts. Then, rather than mandating a particular solution, the market would evolve technology to satisfy the standards and firms could compete to provide the most cost effective security solutions. Thus, systems would be secure from the moment of purchase. To keep the systems secure, software vendors should be held accountable to patch known security vulnerabilities in their software within a reasonable amount of time after discovery. After this time limit expires, the vendor would be liable for damages, thus forcing it to price the externality and modify the calculation of when it is "economical" to correct a problem.

Even with the above measures to provide secure computers, maintaining secure systems requires sound systems administration. Most corporate and government computer systems have a professional system administrator dedicated to ensuring the security of the network, yet almost no home networks have one. To mitigate the risk, ISPs should be held accountable to ensure the proper use of their infrastructure and they should assume some of the traditional responsibilities of a network administrator. Since the U.S. Internet infrastructure is in private hands, policing falls to those hands; the alternative is for the government to police the infrastructure, which most ISPs would find highly objectionable and ripe with opportunity for unintended consequences.

The limited measures proposed would significantly improve network security for a small marginal cost increase. For instance, most ISPs already provide routers to connect their clients; for a nominal marginal cost increase, those routers could be turned into firewalls. This new additional cost must obviously be absorbed by consumers, who would end up paying up front for the security software installed by default on their computers to address the externality. However, even here there is a silver lining: the low marginal unit cost of software combined with the increased volume of security software purchases should enable computer hardware vendors to drive lower prices from security software vendors. As hardware and security software providers compete, savings would be passed on to the consumer who would gain similar security software for less than the cost under the current optional security regime. As previously stated, network security, like defense, is a classic public good externality, but by working together, government and industry can secure the network underpinning our economic engine and increase both consumer and producer welfare. (Lt Col Plaks)

ICT PRIVACY

The balance between the benefits of the interconnected world and threats to privacy from those same technologies creates tension. There can be no expectation of 100% complete privacy once one enters the realm of the Internet and the information age whether at work or at home. Collection and monitoring of information will continue, most with honorable intentions but some not so honorable, with the individual user as the weakest link. Although privacy is a private good, individual consumers have little market influence on privacy protection. Collectively, the government and private industry need to provide a baseline foundation to secure individual privacy and establish an education program to support conscious and informed choices about

which media one uses, what sites one visits, what information one releases and what protection one chooses in hardware and software.

The industry has attempted self-regulation, but efforts are consistent with business objectives and often undervalue consumer privacy. Where the government has stepped in, laws applying to specific industries or practices are enacted in areas like finance and child safety, resulting in a sectoral approach that relies on a mix of legislation, regulation, and self-regulation to protect privacy but still leaves gaps and inconsistencies. Generally, legislation focused on two areas, information security and notification in response to a significant privacy issue or security breach involving personally identifiable information (Stevens 2008). Most consumer advocates insist that this sectoral approach, though appropriate for selected industries and their respective practices, offers little protection for the individual (Givens 2008).

In contrast, European nations, Canada, Australia, New Zealand, and Hong Kong have enacted omnibus data protection laws covering the full spectrum of uses of personally identifiable information in both the private and public sectors (Givens, 2008). The European Commission (EC) directive on data protection created government data protection agencies, which requires registration of databases, and demands prior approval before processing personal data. The EC program, known as Safe Harbor, requires organizations to comply with seven principles to do business in Europe. The seven principles include 1) notification of the purpose and use of data collected (Notice), 2) opportunity to choose whether data can be collected (Choice), 3) transfer requirements to third parties (Onward Transfer), 4) access to information held about them (Access), 5) reasonable precautions to protect information (Security), 6) practices ensuring data is reliable, accurate, complete and current (Data Integrity) and 7) processes to ensure compliance (Enforcement) (Export.Gov 2008).

In the U.S., The Federal Trade Commission (FTC) established five core principles of privacy protection in an attempt to push the industry towards an effective means of self-regulation. These principles are similar to those of the EC Safe Harbor directive (Federal Trade Commission, 2008). Mandatory vice voluntary compliance is required. However, the industry standard for choice is opt-out, allowing automatic data collection until the consumer acts to opt-out of data collection. An opt-in standard would provide more privacy, automatically shielding consumers from data collection until they exercise affirmative steps (opt in) to allow data collection.

As noted, information is collected and monitored continuously. Many consumers lack understanding of the data collected, its accessibility and how long it is retained. Consumer education is imperative. Every user needs to understand what is happening to their information as they engage in the information age. This National Education campaign must be an enduring partnership between industry and government that addresses current and future privacy threats and technologies and uses all available media, non-governmental agencies, schools, state and local governments to inform the population.

The Internet is an integral part of most peoples' lives today. It allows us to find information, manage finances, communicate, shop and socialize. In business, electronic information networks and technology are enablers, providing connectivity globally or just around the corner through computing power, capacity, speed accessibility and cost. Those same characteristics, serving as enablers, pose threats to an individual's privacy. For many, they must decide: stay connected with the associated risks or live unconnected, privacy maintained but removed from a world moving at light speed. Establishing mandatory baseline Internet privacy protection principles, adopting an opt-in vice opt-out choice standard and establishing a National

Internet Privacy Education Campaign would provide consumers of all ages the tools to avoid being the weakest link in the area of privacy. (CAPT Kuzma)

ICT AS AN ENABLER TO U.S. ECONOMIC GROWTH

The ICT sector's contribution to the U.S. economy continues to grow in magnitude and importance thanks to a socio-economic structure that promotes innovation and market participation. ICT products, services and their application are the driving force behind the United States' economic growth of the past several decades. U.S. ICT leadership is hallmarked by innovation and the rapid evolutionary application of information and communication technologies to improve business processes and consumer welfare across the economy. As a result, ICT has motivated a new "information economy" where business models are driven by expertise and intellectual capabilities that are based upon networking, connecting and collaborating (SIIA 2008).

The highest levels of national economic growth are evident in countries where the correlation between applied ICT investment and productivity gains is most significant (SIIA 2008). The U.S. acceleration in economic growth was primarily a result of the large increase in ICT capital. In addition, the U.S. acceleration in labor productivity growth in manufacturing was a result of the ICT producing sectors (SIIA 2008). ICT diffusion has become the critical path to higher productivity and sustained economic growth.

There are specific financial and business characteristics that are best suited to achieve maximum productivity and economic benefit from ICT. Market oriented financial structures with access to large sums of venture capital and a strong entrepreneurial business structure provide the best opportunities to benefit from ICT products, services and their application. Macro level, ICT induced economic growth is strongly influenced by a capital market structure that is both market oriented and possesses a large venture capital market. The U.S. financial and business structures possess these characteristics and have historically been best suited to benefit from ICT diffusion and deepening. Therefore, it is critical that the U.S. maintains this climate of innovation and leadership by fostering strong entrepreneurial market characteristics.

The United States is the leader in developing and providing information and communications technology products, services and their application. The U.S. has experienced a greater than market return for ICT capital over the long run (Matteucci 2005). The ICT sector employs 2.7 million Americans and provides a 17 percent net employment growth between 1997 and 2006 (SIIA 2008). Approximately 11 percent of the growth in GDP is directly attributable to ICT for 2004 and 2005, a growth rate that is three times higher than the U.S. economic growth overall (SIIA 2008). Tremendous future opportunities and challenges exist as the U.S. seeks to improve the way we digitize, move, process, and display information. Consumer demands and expectations are rapidly driving innovation and are increasing the depth, breadth and quality of the human experience with information throughout business, government and society. U.S. consumers and businesses have an insatiable demand for broadband and wireless expansion and corresponding development in e-commerce, e-banking, e-government, e-education, and e-health.

The ICT revolution can be viewed as a large and long-lasting positive supply shock, creating higher and possibly more stable economic growth without extra inflation (Houben, 2002). Unlike many other countries, the U.S. benefits from market focused venture capital investment in young start-up entrepreneurial businesses, which enables the momentum of ICT innovation. Barriers to trade, such as the Berry Amendment and International Traffic in Arms Regulations, fundamentally limit the United States' ability to compete in the global market and

must be dramatically altered to preserve U.S. economic growth potential. Enabling and enhancing ICT innovation – the quintessential American hallmark – must be recognized as a U.S. national economic priority. (COL Claflin)

SOFTWARE ON DEMAND/SOFTWARE AS A SERVICE

Software as a Service (SaaS) is a growing class of software applications that provide services to businesses and individual consumers. Software as a Service provides hosted software applications to end users via the Internet, generally on a subscription basis. In the current market, business applications focus on customer relationship management, analysis and generic business functions. Examples of applications designed for individuals are tax preparation, word processing and entertainment software. There are many firms developing applications for the SaaS market; they have migrated from venture capital start-ups to major software powerhouses over the last ten years as the market has evolved. A reason major software companies entered this market is that increased broadband Internet deployment provides reliability and data security to the point where customers are comfortable with the concept of using remotely hosted applications. Customer comfort has manifested into increased use of SaaS applications and market experts predict significant future demand for this class of software product.

Multiple sources, including *Springboard Research*, predict SaaS applications will grow substantially through 2010 and reach a value of $11.5 billion in 2011 (The Economist 2008, 1). Given predictions of an expanding market, smaller software development firms are developing specific applications and larger firms are either buying existing companies or building internal capabilities to develop enterprise SaaS solutions to capture market share.

The SaaS market is still maturing and may eventually become the application deployment standard for general service applications across the globe. The current major market, however, is small to medium businesses and individual consumers. Large business purchasing trends indicate they intend to maintain control of software applications and will not consider SaaS applications until after existing intranet hardware and software applications fully depreciate and/or become too costly to maintain (Whiting 2006, 24).

Businesses providing software products are adjusting research and development portfolios and business models based on these emerging market trends. Google, Oracle, SAP, Sun Microsystems and Microsoft are developing enterprise SaaS solutions for business and individual consumers. These economic and market factors are moving the market towards an oligopoly structure. There are a limited number of developers with sufficient scale in terms of capital, personnel and hardware infrastructure to effectively develop, deploy and host competitive SaaS applications that yield a quality customer experience. With five major companies jockeying for greater market share, it is just a matter of time before they capture over 40% of the available market. Sufficient competition should remain, however, to ensure relative price equilibrium for basic SaaS applications that will set consumers up for the next wave of affordable and productive applications. (COL O'Donell)

INTELLECTUAL PROPERTY RIGHTS

Key U.S. copyright-based industries, which include a major portion of the ICT industry, accounted for an estimated $819 billion or 6.56% of the U.S. GDP in 2005 (Smith 2008, 2). ICT industry firms provide a broad array of technologically advanced, innovative products, services and solutions to numerous industry organizations and consumers. A large part of ICT firms' success is dependent on their ability to develop intellectual property (IP) and leverage that IP for

producer and consumer economic benefit. Despite these successes, threats to U.S. creators and the ICT industry abound largely from patent system deficiencies, copyright enforcement challenges, rampant piracy, and the failure of governments to enforce IP laws effectively.

Copyright violations worldwide pose serious threats to the ICT industry and have cost the U.S. billions of dollars in lost sales over the last few years with these losses impacting future possible R&D revenues. An estimated trade loss due to copyright piracy for business software alone was $12.9 billion in 2007 (Smith 2008, 18). U.S. government efforts in promoting copyright reform play a key role in protecting and enforcing IP rights by taking action against those accused of theft or misuse.

While the Internet vastly increases opportunities to research, market, and sell products and services, it also creates new and relatively easy opportunities to steal IP, such as software. Corporate piracy of business software and digital content is a leading cause of lost revenue within the industry and unfortunately, this trend is increasing. According to an IDC report released in 2007, the software industry lost $28.8 billion worldwide due to piracy occurring within corporations and other organizations (SIIA 2007). Industry trade organizations like the Software & Information Industry Association (SIIA) and the Business Software Alliance (BSA) are leaders in the fight against piracy. SIIA and BSA employ strict Corporate Anti-Piracy programs to minimize and discourage software piracy in the workplace.

Efforts to reduce piracy and increase and enhance IP protection enforcement within the ICT industry must continue to assure future innovation. Advances in new technologies are dependent upon strong intellectual property protection and innovative solutions to enhance that protection. Patent system reforms are necessary to maintain U.S. technological advances and competitiveness. Fortunately, innovations under development today will serve to protect companies from future piracy threats. Identifying additional ways to leverage market forces to solve these problems and using patents to encourage cooperation vice disputes are key ingredients for future industry success. Finally, governments need the political will to take responsibility to address copyright enforcement meaningfully, continue steps to reduce piracy, and facilitate open markets, which ultimately benefit the global ICT industry. (LTC Williams)

HUMAN CAPITAL

We will lose our technological and innovative advantage if we do not continue to grow and nurture highly educated and inventive professionals in the U.S. to compete in the global economy. In the ICT sector, “The Bureau of Labor Statistics’ 10-year economic and employment predictions, released 4 Dec 07, show that the computer professionals’ job market is expected to grow at a record pace through 2016. From 2006 to 2016, network systems and data communications professionals will make up the single fastest-growing occupation, increasing by an estimated 53.4%” (Perelman 2007, 1). Many companies claim they offshore to find qualified personnel while others believe companies offshore for purely economic reasons – reduced salary costs. However, in reality both are occurring in a highly competitive global market for ICT professionals. Although the number of engineering college graduates in the U.S. has increased from 1999 to 2006, both India and China have increased at a higher rate as shown in Table 1 below. ICT firms are therefore moving more jobs to where the ICT labor is available.

Graduates in Engineering, Computer Science, and Information Technology			
Bachelors Degrees	1998-1999	2005-2006	Percent Increase
United States	103,000	129,000	25%
India	68,000	220,000	224%
China		575,000	
Graduate Degrees	1998-1999	2005-2006	Percent Increase
United States	39,525	50,585	28%
India	4,500	20,000	344%
China	15,391	82,386	435%
Ph.D Degrees	1998-1999	2005-2006	Percent Increase
United States	6,100	8,887	46%
India	650	700	8%
China	4,000	12,130	203%

Table 1. (Gerefifi, Wadhwa, Rissing, Ong 2008, 19).

The number of graduates in the United States is also misleading. As shown in Table 2, foreign nationals make up a significant portion of U.S. college graduates. This is not an issue if these individuals are allowed to remain in the U.S., but tightened immigration rules since 2001 have made this increasingly difficult.

Percent of U.S. Engineering degrees earned by Foreign Nationals					
United States	**1998**	**2000**	**2002**	**2004**	**2005**
Bachelors Degrees	**7.8%**	**7.5%**	**7.7%**	**7.5%**	**7.2%**
Graduate Degrees	**39.7%**	**43.0%**	**46.0%**	**42.6%**	**39.8%**
Ph.D. Degrees	**45.6%**	**53.8%**	**55.2%**	**59.4%**	**61.7%**

Table 2. (Gerefifi, Wadhwa, Rissing, Ong 2008, 19).

As the economies in India and China expand, the number of ICT jobs will also increase to support their own infrastructure. Therefore, we must take action now to ensure the U.S. maintains its competitive edge in ICT. Increasing the number of qualified engineers or computer scientists will not occur overnight. We must look at the short and long-term solutions to this issue. Perhaps the short-term fix is to ensure foreign nationals are allowed to remain in the U.S. to work after they earn their degrees. This would involve increasing the number of H-1B or work visas allowed annually. The long-term fix is the most difficult. Although we may not be in imminent danger of losing all our jobs to India and China, we certainly must take charge of our education system to ensure our children are studying STEM disciplines. Increasing scholarships, restructuring school loans, and establishing industrial partnerships with schools are some ways to counter the decreasing U.S. STEM graduates. The U.S. government cannot tackle this issue alone; industry must also take responsibility to ensure the education system produces the type of individual they are seeking in the future. (Ms. Lasichak)

INTERNATIONAL OBSERVATIONS

As noted in surveys of the United Kingdom, Africa, and Korea and in international travels to China, dial-up, broadband, and mobile Internets are the main methods for staying connected. With the exponential explosion of mobile phone and Internet subscribers, the ICT

industry is becoming the most dynamic sector in these economies. Users have increasingly switched from dial-up to broadband and the trend is expected to continue. A major task will be to continue upgrading mobile Internet related content, infrastructure, services, and applications. ICT infrastructure has improved substantially in recent years, thanks to the implementation of a number of ICT-related government programs. The lack of competition among telecom and entertainment providers, opposite of what has been seen in the U.S., has limited the need for faster services or higher bandwidth in these regions. Download and upload speeds appear to be much slower than those seen in the U.S. with little evidence of demand for higher speeds by consumers. While Taiwan and mainland China have extensive fiber backbones, the last mile is mostly DSL. Consumers pay minimal rates and receive basic services.

Regulatory issues identified in these surveys show barriers to rapidly improving ICT growth. For example, China faces a long list of issues. Some of the most important include the issuance of 3G mobile phone licenses, restructuring of the six state-owned telecom operators, development of and consensus on domestic technology standards, opening of the market to foreign telecom operators, development of a system for universal service, and the control and censorship of content and applications offered over fixed-line and mobile telecom networks.

Competition and relaxed government oversight will be key to China's ICT industry to maintain its current growth rate. Many Chinese officials recognize the need for more competition to enable future growth. Higher data rates will be important as high definition and 4G communications systems come on line. Although ADSL is sufficient today in the countries surveyed, this infrastructure will not support the future convergence of IP and broadband solutions such as voice, data, and streamed multimedia. Cable TV could offer a future alternative but, for the present, it remains walled off from China's ICT industry for public policy reasons. (Mr. Ramsey)

CONCLUSION:

The Information and Communications Technology industry is critical to the continued prosperity, growth, and security of the United States. ICT is a major source of American economic strength, both as a direct export and as an enabler for efficient operation of other industry sectors.

ICT remains the fastest growing sector of the U.S. economy. The future of the Internet is mobile, convergent, and centralized. Voice, video, and packet data are becoming increasingly interchangeable, with fewer distinctions between telecommunications firms and cable television providers. Fiber optic backbones provide greater bandwidth, with a larger amount of mobile wireless coverage branching off from this core. Competition to deliver bandwidth will increase as telecommunications, wireless, and cable firms overbuild each other's networks. Economies of scale for data management will promote SaaS and centralization of computing power, enabled by higher network speeds and the proliferation of wireless devices. Security of information and identity will become more critical as personal, corporate, and governmental transactional processes aggressively shift towards the vulnerable virtual domain. The U.S. ICT industry will continue to face significant obstacles to achieving consensus on the right blend of open market principles and regulation that will maintain U.S. leadership.

Governments have historically played significant roles in balancing the requirements of individuals, firms, and society. The U.S. faces challenges that threaten its ability to maintain ICT-derived economic preeminence and command and control in the event of a cyber attack,

terrorist attack, natural disaster or other disruptive incident, which could damage the nation and potentially threaten its sovereignty. To continue to spur growth and innovation while benefiting consumers and defending the nation, the federal government should limit ICT industry regulation to inherently governmental issues, adopting the following policies.

First, the U.S. should adopt a policy of relaxing overt telecommunications regulation and opt for a more incentive-based policy approach that promotes competition, private ownership, and market forces. Second, to improve interoperability of public safety communications, the government should define and mandate technology standards such as Project 25. Third, the government must coordinate with the private sector and other nations to update laws and agreements that prevent and respond to ICT-related malfeasance, which has the potential to harm American and worldwide economic strength and cripple key sectors of national infrastructure. This will require a national dialogue on the civic responsibilities of end users, firms, and governments as they participate in a networked society. Fourth, the government should collaborate with the private sector to rejuvenate the ICT workforce by retaining foreign workers and incentivizing STEM education for U.S. citizens. Finally, the government should not enact wireless network neutrality rules. Although there are multiple proposals and definitions, most approaches represent a form of rent seeking by the content industry, and would represent a return to the common carrier era under the Bell System. Instead of mandating network neutrality, the FCC should adopt policies designed to improve ICT competition.

The ICT industry began to grow deep roots in the U.S. over two decades ago given world-class research universities, extensive and available investment capital and a financial structure that encouraged and rewarded the "American" entrepreneurial spirit. However, as a knowledge-based, readily digitized industry, it is mobile by its very nature and free to move offshore, should the government adopt shortsighted or counterproductive policies. Therefore, we must preserve the positive factors that created the industry while addressing the challenges facing this sector. By anticipating and responding to changing trends in the industry and society responsibly and appropriately, the U.S. Government can ensure that America continues to maintain its ICT leadership, economic growth, and ultimately its national security.

References

America Online/National Cyber Security Alliance. "Online Safety Study." December 2005. http://www.staysafeonline.info/pdf/safety_study_2005.pdf/.

Amobi, Tuna N. and Eric Kolb. "Broadcasting, Cable, and Satellite." *Standard and Poor's Industry Studies*. 175, no. 50 (December 13, 2007). http://www.netadvantage.standardandpoors.com.

Arquilla, John and David Ronfeldt. *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica: The Rand Corporation, 1999.

Bright, Arthur. "Estonia Accuses Russia of 'Cyberattack'." *The Christian Science Monitor*. (2007). http://www.csmonitor.com/2007/0517/p99s01-duts.html/.

Broache, Anne. "Bill Gates to Congress: Let Us Hire More Foreigners." *C/Net News.Com*. March 12, 2008. http://www.news.com/8301-10784_3-9892046-7.html/.

"Business: A question of demand; Software as a Service." *The Economist*, January 5, 2008, 58.

Cashell, Brian, William Jackson, Mark Jickling, and Baird Webel. *The Economic Impact of Cyber-Attacks*. Washington, D.C.: Congressional Research Service, 2004.

Cathers, Dylan, "Computers: Commercial Services," *Standard and Poor's Industry Studies*. 176, no. 18 (November 1, 2007). http://www.netadvantage.standardandpoors.com.

Cord, Erritt. "Cloud Computing is Here." *ECord*. Jan. 2008. http://www.ecord.us/articles_cloud_computing.php.

CTIA. "U.S. Wireless Industry Overview," Lecture to Industrial College of the Armed Forces, Washington, D.C. March 14, 2008.

Drennan, Matthew P. *The Information Economy and American Cities*. Baltimore: The Johns Hopkins University Press, 2002.

Export.Gov. "Safe Harbor Overview". http://www.export.gov/safeharbor/SH_Overview.asp.

Federal Communications Commission. "Wireless Auction 73—700MHz Band Fact Sheet." http://wireless.fcc.gov/auctions/default.htm?job=auction_factsheet&id=73/.

Federal Trade Commission. "Privacy Initiatives." http://www.ftc.gov/privacy/.

Gansler, Jacques S. and Hans Binnendijk. *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. Washington, D.C.: National Defense University, Center for Technology and National Security Policy, 2004.

Gereffi, Gary, Vivek Wadhwa, Ben Rissing, & Ryan Ong. "Getting the Numbers Right: International Engineering Education in the United States, China, and India." January 2008. http://ssrn.com/abstract=1081923.

Givens, Beth. "Privacy Expectations in a High Tech World." Opening presentation, symposium on Internet Privacy, Computer and High Technology Law Journal, Santa Clara University, February 11-12, 2000. http: //privacyrights.org/ar/expect.htm.

Government Accountability Office. *FIRST RESPONDERS: Much Work Remains to Improve Communications Interoperability*. Washington, D.C.: United States Government Accountability Office, 2007. http://www.gao.gov/new.items/d07301.pdf.

Houben, Aerdt and Jan Kakes. "ICT Innovation and Economic Performance: The Role of Financial Intermediation." *KYKLOS* 55 (2002).

Jacobs, Eva E. and Mary Meghan Ryan, eds., *Handbook of U.S. Labor Statistics: Employment, Earnings, Prices, Productivity, and Other Labor Data*, Lanham, MD: Bernan Press, 2006.

Juster, Kenneth. *Economic Security and Critical Infrastructure Protection*. New York: U. S. Bureau of Industry and Security, May 22, 2002.

Khalil, Chris. "Software as a Service." *The Future of Software Apps*. April 2, 2007. http://www.chriskhalil.com/2007/04/02/software-as-a-service-the-future-of-software-apps/

Martikainen, Olli. *ICT and Productivity*. Finland: The Research Institute of the Finnish Economy, December 13, 2007.

Matteucci, Nicola, Mary O'Mahony, Catherine Robinson, and Thomas Zwick. "Productivity, Workplace Performance and ICT: Industry and Firm-Level Evidence for Europe and the U.S." *Scottish Journal of Political Economy* 52, no. 3 (July 2005): 359-386.

National Telecommunications and Information Administration. *Networked Nation: Broadband in America 2007*. Jan. 2008. http://www.ntia.doc.gov/reports/2008/NetworkedNationBroadbandinAmerica2007.pdf

Organization for Economic Cooperation and Development. *OECD Information Technology Outlook 2006*. Paris: OECD, 2006.

Organization for Economic Cooperation and Development, *Measuring the Information Economy*. Paris: OECD 2002. http://www.oecd.org/document/5/0,3343,en_2649_33757_2765701_1_1_1_1,00.html

Perelman, Deborah, "*Tech Job Sector Growing at Record Paces Through 2016,*" December 6, 2007. http://www.careers.eweek.com/c/a/news/Tech_Job_Sector_Growing_at_Record_Paces_Through_2016/.

Razavi, Bezhad. “Gadgets Gab at 60 GHz.” *IEEE Spectrum* (February 2008). http://spectrum.ieee.org/feb08/5916/.

Rosenbluth, Todd “Telecommunications: Wireline,” *Standard and Poor’s Industry Studies*. 176, no. 6, (February 7, 2008). http://www.netadvantage.standardandpoors.com/.

Rosenbluth, Todd and Karen Kawaguchi”Telecommunications: Wireless,”*Standard and Poor’s Industry Studies*. 175, no. 40 (October 4, 2007). http://www.netadvantage.standardandpoors.com/.

Sharma, Amol. "Cell Firm's Shutdown may Crimp FCC Plan." *Wall Street Journal.* January 9, 2008. http://www.freepress.net/news/29428.

Smith, Brenna and Tom Tolman. "Can We Talk? Public Safety and the Interoperability Challenges." *National Institute of Justice Journal* 243 (April, 2000),17.

Smith, Eric H. *IIPA Special 301 Letter to USTR. 2008.* http://www.iipa.com/pdf/2008SPEC301COVERLETTER.pdf/.

Software & Information Industry Association. Presentation to Industrial College of the Armed Forces, Washington, DC, February 25, 2008.

Software & Information Industry Association (SIIA). *SIIA Anti-Piracy: 2007 Year in Review*. 2008. http://www.siia.net/piracy/yir_2007.pdf/.

Stevens, Gina Marie. *Information Security and Data Breach Notification Safeguards.* http://www.fas.org/sgp/crs/secrecy/RL34120.pdf/.

Tasker, Joe and Trey Hodgkins. Presentation to the Industrial College of the Armed Forces, Rosslyn, VA, March 6, 2008.

The Rand Corporation, *The Global Technology Revolution 2020, In-Depth Analysis,* 2006. http://rand.org/pubs/technical_reports/2006/RAND_TR303.pdf/.

U.S. Department of Homeland Security. "About SAFECOM." http://www.safecomprogram.gov/SAFECOM/about/default.htm/.

U.S. House of Representatives. 2007. Sub-Committee on Immigration, Citizenship and International Law. *Comprehensive Immigration Reform: a Business Perspective*. Washington, DC: Government Printing Office, 2007.

Whiting, Rick. “Look no Software; Industry Veteran Dave Duffield Brings New Credibility to Software as a Service, but ERP may be a Hard Sell.” *Information Week*, November 6, 2006: 24.