Spring 2017
Industry Study

Final Report
Information and Communications Technology

CLEARED
For Open Publication

AUG 17 2017

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

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

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) 2017

ABSTRACT: The Information and Communications Technology (ICT) industry is evolving at a rapid pace while serving as a catalyst for digital entrepreneurship in a new data-driven world interconnected via the internet and cyberspace. ICT supports and enables the day-to-day operation of modern societies, while providing newfound opportunities for economic growth through digital trade. In order to maintain the ICT industry's steep growth trajectory, policymakers must focus on three areas: (1) cybersecurity to protect increasingly vulnerable critical infrastructure; (2) privacy to protect citizens' rights in an age of data collection and exchange; and (3) the growing shortfall of technology workers needed to maintain innovation leadership.

CDR Christopher Biggs	U.S. Navy
Mr. Charles Day	Department of the Army
Lt Col Tony England	U.S. Air Force
Ms. Sheila Harris	Office of the Secretary of Defense
LTC Bennett Hayth	U.S. Army
Ms. Kelli Lozada-Reese	Intelligence Community
Mr. Norbert Marcelle	Department of Energy
COL Marcos Antonio Martins da Silva	Brazilian Army
CAPT Stephen McKone	U.S. Navy
Mr. Donn Murakami	Department of the Navy
COL Antonio Ralph	U.S. Army
Lt Col Rodney Stevens	U.S. Air Force
LTC Brady Stout	U.S. Army
COL Nicolas Tessaud	French Defense Procurement Agency (DGA)
COL James Walsh	U.S. Army

Col Paul Gillespie, PhD	U.S. Air Force, Faculty Lead
Mr. Richard Altieri, J.D.	Faculty
Mr. Stephen Bloor, J.D.	Faculty
Mr. John Beed	Faculty
Dr. Todd McAllister	Faculty

Industry Study Outreach and Field Studies

On-Campus Presenters

John Kneuer, Federal Communications Commission
Ron Repasi, National Telecommunications & Information Agency
Elaine Wu, U.S. Patent & Trademark Office
David Holtzman, Author, GlobalPOV
Greg Myers, Microsoft
Dr. Brad Lackey, University of Maryland
James Ittenbach and Gary Katz, DoD Cyber Crime Center
John Backus, NAV Venture Capital
Chris Algiere, FirstNet

Field Studies—Domestic

Information Technology Industry Council (ITIC), Washington, DC
Software & Information Industry Association (SIIA), Washington, DC
Cellular Telecommunications and Internet Association (CTIA) – The Wireless Association, Washington, DC
International Business Machines (IBM) Federal, Washington, DC
National Cable & Telecommunications Association (NCTA) – The Rural Broadband Association, Washington, DC
Verizon, Ashburn, VA
American Telephone and Telegraph (AT&T), Washington, DC
National Security Agency (NSA), Ft. Meade, MD
U.S. Cyber Command (USCYBERCOM), Ft. Meade, MD
Laboratory for Telecommunication Sciences (NSA), College Park, MD
Department of Homeland Security, Arlington, VA
Defense Information Systems Agency, Ft. Meade, MD
Cisco, San Jose, California
FireEye, Milpitas, California
Facebook, Menlo Park, California
Google, Mountain View, California
National Aeronautics and Space Administration (NASA) Ames Research Center, Moffett Field, California
Oracle, Redwood City, California
Shape Security, Mountain View, California

Field Studies—International

IngDan, Shenzhen, People's Republic of China (PRC)
Genvict Technology, Shenzhen, PRC
Zhongxing Telecommunication Equipment (ZTE), Shenzhen, PRC
HAX, Shenzhen, PRC
BYD, Shenzhen, PRC
Hong Kong University of Science and Technology, Hong Kong, PRC
Shangri La Hotels, Hong Kong, PRC
Applied Science and Technology Research Institute (ASTRI), Hong Kong, PRC
Vision 2047, Hong Kong, PRC
U.S. Consulate General, Hong Kong, PRC
Dr. Séverine Arsène, French Centre for Research on Contemporary China, Hong Kong, PRC
American Chamber of Commerce, Hong Kong, PRC
Pacific Century Cyber Works (PCCW), Hong Kong, PRC

Introduction

Today, information and communications technology (ICT) connects over 60 percent of the world's population to digital markets, schools, governments, and each other.[1] The ICT industry has spurred economic growth in ways that were unimaginable when the first computers were connected with a dial-up telephone connection in 1965. It is not only the production and sale of ICT goods and services that have driven economic growth, but also the internet, the broader cyberspace domain, and the data that ICT and the internet have made available that has enabled a new age of digital entrepreneurship.[2]

In addition to opening new economic possibilities, ICT enables a cyberspace that provides critical capabilities impacting nearly every institution in modern societies, to include critical infrastructure, data and information management, distributed learning, global logistics, military command and control, and much more. Considered as a global common, access to and freedom of movement within the cyberspace domain are critical to the national security of the United States (U.S.), its allies and partners, with direct impact to U.S. strategic objectives to: (1) strengthen U.S. national defense, (2) put the U.S. economy to work; (3) enable the U.S. to lead in science, technology, and innovation; (4) shape the global economic order; and (5) enable the U.S. to live its values, such as free speech, free access to information, and equality.[3]

The Eisenhower School's ICT Industry Study (IS) analyzed various aspects of the ICT industry. The IS reviewed today's technology trends, such as cloud computing, the Internet-of-Things (IoT), and big data, as well as game-changing technological capabilities on the horizon, such as artificial intelligence (AI) and quantum computing. The IS also explored the human dimension of the ICT industry, arguably the most critical element in a world of machine learning and digital assistants. Lastly, the IS analyzed the policy implications of today's ICT-driven world in terms of impact to the digital economy; the need to acquire a new generation of technology-oriented workers; the growing exchange of information and data, and related privacy concerns; and implications to national security. This paper provides the ICT Industry Study's analysis of the industry along with additional insight into specific areas that warrant added focus from national leadership and decision makers.

The Industry Defined

Overview. Economists define markets by the interactions of buyers and sellers which, in the case of ICT, covers a broad swath of the global economy. Defining the markets within the ICT industry is complicated by the ubiquitous nature of information technology products, speed of product innovation, and ease with which consumers are able to migrate from one firm or product to the next. These ICT industry products span a broad range from wearable devices feeding consumers information on a range of environmental and personal factors, to encryption capabilities, which provide virtually unbreakable security to everyday communications, to the vast data processing and storage potential of cloud computing services, to the nearly unimaginable computing power promised by tomorrow's quantum computers.

Demand in the ICT marketplace is divided into two distinct areas: (1) individual consumer demand and (2) business demand. Consumer demand is driven by increased consumer confidence and by a variety of factors such as falling prices due to the impact of Moore's Law in driving technology innovation at an ever-increasing rate along with strong competition between firms.

On the other hand, business demand is driven by the continuous efforts to increase efficiency and lower costs. It is also expanding as profits increase and firms recover from the 2008 economic slowdown.

For this essay, the ICT IS chose to divide the U.S. market into four key areas based on Computing Technology Industry Association's (CompTIA) 2017 Industry outlook report and current IBISWorld Industry North American Industry Classification System (NAICS) research reports.[4] In their 2017 industry outlook paper, CompTIA reported that, in 2016, the global information technology (IT) industry exceeded $3.4 trillion with the U.S. market accounting for over $1 trillion.[5] In the global market, industry services accounted for 19 percent of total revenues, hardware 27 percent, software 13 percent, and telecommunication services accounted for the remaining 41 percent. A detailed breakout of the NAICS reports associated with the individual market segments is located in Appendix 1.

IT Services. The IT services industry segment reflects the planning, management, and support of the broader ICT industry. More broadly, it encompasses internet publishing and search engine firms. It is comprised of a large number of highly competitive firms with moderate but growing barriers to entry. Despite growing revenues, U.S. firms face significant threats from foreign competitors. The Everest Group named Cognizant, Accenture, and IBM as the top firms of 2016.[6] Alphabet and Facebook are the leading firms in the internet publishing and search engine aspects of this market segment.

Hardware. The hardware segment is comprised of the physical components of a network and is largely defined by the manufacture of semiconductors, computers and servers, voice and data equipment, telephone and internet protocol-based switching systems, cell phones, antennas and satellite uplink equipment. The industry is comprised of a small number of large firms, but remains highly competitive with high barriers to entry. Despite growing consumer and business demand, this market segment has struggled with profitability over the past five years due to price pressures imposed by imports from Asia, namely China. Leading U.S. firms in this industry segment are: Cisco, Hewlett-Packard (HP), Harris, Dell, and IBM.[7]

Software. The software industry segment is comprised of many firms of various sizes and is competitive in nature with moderate barriers to entry. The industry is defined by the data and instructions that enable computers to function and is generally broken into two categories: system and application software. System software operates the hardware and services the application software operating on the computer. Application software is how users interact with the system to execute tasks. Leading firms in this industry segment include Microsoft, Apple, IBM, Oracle, Hewlett-Packard Enterprise Company, and Forensic Technologies International Consulting, Inc.[8]

Telecommunication Services. This is the largest segment of the industry and is comprised of a large number of highly competitive firms with strong barriers to entry. U.S. Code Title 47, Chapter 5, Subchapter I, Subsection 153 defines telecommunications and telecommunications service as simply the transmission, for a fee, of information between or among points specified by the user.[9] In that light, this market segment is comprised of the wired and wireless network switching and transmission facilities that enable mobile and fixed point internet access. The segment also includes substitute products such as voice over internet protocol (VoIP) services and satellite telecommunications providers and companies focused on reselling telecommunications services. The key firms in this market segment include AT&T, Verizon Communications, Deutsche Telekom, Sprint, América Móvil, and Vonage Holdings.[10]

The Current Condition of the Industry

As a general-purpose technology, the impact of the various firms within the overall ICT industry extends well beyond productivity gains.[11] Many of the firms are vectors of economic and social transformation through improving access to services, enhancing internet access, and creating new businesses, as well as employment opportunities.[12] This tends to change the ways people communicate, interact, and engage with each other, as well as with their governments.[13] Such a diverse industry can be difficult to map out and even more difficult to determine an accurate representation of its current and future health. The ICT industry occupies different categories within the market competition spectrum due to the diversity of the industry, which focuses on the four key areas of hardware, software, services, and telecommunications.

Hardware & Software. The current trend in ICT for hardware and software is virtualization, cloud computing, and software-defined networks. This has created a significant reduction in hardware revenue while at the same time creating growth in software sales. Additionally, companies such as IBM, HP, and Dell are experiencing sales slumps in their server markets, but strong sales for personal computers (PC) and other similar devices.[14] The worldwide server market has declined by an average of 7 percent annually to $12.5 billion in the third quarter of 2016.[15] The stagnation in the server market is due mostly to slow growth of data centers and a push to cloud computing that further reduces revenue from traditional data center operations and maintenance costs.[16] However, the cloud trend may also increase hardware revenues for some vendors since many enterprises are building private clouds and larger cloud providers require hardware as well.[17] But both virtualization and software defined networks ultimately allow organizations to do more with less, thus reducing the need for hardware while increasing or sustaining the requirements for software.[18]

IT Services. IT security consulting is performing well in all business sectors, including banking and financial services, telecommunications and retail, and continues to react proactively to the risk of high-profile, reputation-threatening breaches. In 2016, the Department of Homeland Security's U.S. Computer Emergency Readiness Team reported 33,632 cybersecurity incidents.[19] With revenue at $11.6 billion in 2016, the growing prevalence of high-profile cybersecurity attacks and the risks associated with potential data breaches (coupled with losses due to cybercrime expected to "cost the world in excess of $6 trillion annually by 2021")[20] will continue to propel the services forward. As demand increases, new companies are likely to enter the market with service participation levels expected to rise an annualized 2.4 percent to 4,590 businesses over the next five years, and overall revenue is expected to grow an annualized 5.7 percent to $15.3 billion.[21]

Data processing and hosting services are one of the fastest-growing subcategories. These services continue to fare very well with revenue increasing by 11 percent in 2016.[22] Over the next five years, revenue for these services is expected to grow at an annualized rate of 4.8 percent to $182.3 billion.[23] Many companies have cut internal IT management, outsourcing work and utilizing cloud computing services to reduce business costs. Cloud computing has quickly become one of the fastest-growing markets with countless companies offering this service. As the technology required for data processing and host services becomes more complex, the level of expertise needed to effectively manage large data centers will continue to rise. This service is moving towards independent contractors and large companies to meet the computing demands of clients.

Cloud computing has impacted individual consumers for some time through its leveraging of the internet.[24] However, business and government are just starting to leverage cloud computing

services in order to gain cost savings from reduced operations and management costs of expensive on-premise data and computing centers. According to the National Institute of Standards and Technology (NIST), "cloud computing is a model for enabling ubiquitous, 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 and released with minimal management effort or service provider interaction."[25] The NIST definition identifies five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service.[26] NIST also lists three service models: software, platform, and infrastructure as a service and four deployment models: private, community, public, and hybrid cloud that combine together to categorize and determine different ways to deliver cloud services.[27]

The ICT Industry uses the terms data analytics and big data to describe an emerging market that leverages large volumes of both structured and unstructured data that typically inundates business systems on a day-to-day basis.[28] It is not the amount of data that is important, but rather how the data is used and the analytics that are performed against the data that matters.[29] The current trend in ICT is to create ways to analyze large data sets and create insights that lead to better decisions and strategic business moves.[30] During 2016, big data initiatives became more mainstream rather than cutting-edge technology with many organizations' Chief Information Officers leading efforts that went well beyond what they dreamed possible a decade ago.[31] Now that data analytics and big data initiatives are becoming more mainstream, organizations in the ICT industry are starting to target the next frontier–how to transform large data sets into products and services that generate revenue.[32] Big data will be explained in more detail in the Major Issues portion of this document.

One subset of IT services is internet publishing and search engine services that provide services such as webpage publishing and access to internet search engines like Google or Microsoft's Bing. There is potential for continued growth opportunity in the internet publishing and search engine industry because of increasing worldwide internet penetration rates and increasing individual usage times.[33] Firms who operate in these industries will continue to see growth opportunities over the next five to ten years.[34] One primary drive is the penetration of the internet into developing countries and the increasing number of internet access platforms that continue to bring in millions of new users, attracting more advertisers and other potential revenue streams.[35]

Telecommunications Services. ICT is an umbrella term that includes any communication device or application that encompass radio, television, cellular phones, computer and network hardware/software, satellite systems, and so on. ICT is playing a vital role in the extension of IoT, which is connecting devices over the internet using applications and software to include viewing motion-sensing camera systems, monitoring healthcare devices for the human body, and regulating irrigation of crops. IoT has become a central part of modern life with industry assessments estimating approximately 50 billion devices being connected to the internet by 2020[36] and another 500 billion devices by 2030.[37] This multitude of internet-connected devices has presented hackers a new attack vector to infiltrate networks. Due to the wide range of devices and technologies, it has thus far been difficult to implement a cohesive security strategy to counter this threat.[38]

The subcategory of wireless telecommunications has performed very well with growth of 3.2 percent to a worldwide total revenue of $1.73 trillion in 2016.[39] Companies in developing countries are starting to gain the benefits of having rolled out fourth-generation (4G) networks and continue to increase subscribers. Over the next five years, fifth-generation (5G) networks are

also expected to take shape with a significant chance of expanding operations. Additionally, the subcategory of satellite telecommunications revenue experienced a growth of 2.5 percent in 2016.[40] The demand for satellite telecommunications remains high with new markets constantly emerging. New high throughput satellites are expected to boost satellite operators' bandwidth capacity, increasing coverage offerings and lowering product prices to compete with other forms of telecommunication.[41] Revenue is forecast to grow an annualized rate of 3.2 percent to $8.5 billion with investment in new technologies to gain an advantage in the next five years.[42] The subcategory of wired telecommunications is expected to continue focusing on and expanding in-demand services such as high-speed internet. Wired telecommunications is expected to see a decline of 1.8 percent in 2017.[43] In the next five years, it is estimated that revenue will decline at an annualized rate of 1.6 percent to $153 billion as demand for voice services continues to decrease with a greater percentage of households using only wireless phones.[44] The U.S. and foreign wired markets are struggling to remain relevant against competing technologies.

Industry Challenges

Cybersecurity. The internet has become the primary information and telecommunications platform of the modern era, and cybersecurity is of utmost concern to the ICT industry. Dominant players such as Amazon, Oracle, Microsoft, and Google have migrated toward cloud computing architectures to manage increasingly large data sets and data flows between an expanding set of users and internetworked devices. As a result, protecting these large datasets has become an even greater challenge, with severe and strategic implications. Simultaneously, and as previously mentioned, the IoT is upon us, with the number of internet-connected devices projected to reach 50 billion by 2020.[45] As both government and industry move toward cloud storage, and as consumers increasingly embrace the IoT, society will expose an ever-widening attack surface to those that may want to exploit cybersecurity vulnerabilities.

Risk can be defined by threats, vulnerabilities, consequences, and mitigation strategies.[46] Given the unprecedented amount of risk created by the ICT industry's lack of incentive for creating secure products, the general public's lack of cybersecurity knowledge, and the increasing complexity of cyberspace threats, there is general consensus that cybersecurity strategies must be enhanced. The defense industrial base (DIB) has faced many cybersecurity threats with regard to its capability to protect classified and sensitive unclassified data. State and non-state actors increasingly challenge both government and commercial information systems, with an alarmingly high and increasing rate of stolen user credentials.[47] As a result, there are an increasing number of consequences to consider, including disclosure of classified information and violations of personal privacy.

Immediate steps should be taken to mitigate cybersecurity threats posed by state and non-state actors against both public and private systems. A multitude of government agencies are charged with protecting cyberspace, and often times, these agencies operate in isolation and work duplicatively. In the defense security environment, clear policy that defines who is responsible and accountable when it comes to managing cybersecurity issues is required. Federal agencies charged with cybersecurity must integrate to allow a free flow and exchange of information to increase overall synergies. Such integration should extend to cleared defense contractors to further strengthen cybersecurity. Additionally, both government and industry must strengthen defenses and protect against stolen user credentials.

Given the dynamic nature of the ICT market, the DIB must establish productive partnerships with world-class cybersecurity firms. Such partnerships will allow for the

development of products and solutions to counter emerging threats in cyberspace and will foster productive and enduring relationships with those at the edge of innovation.

Privacy. Digital privacy is an issue that has received attention from both the public and private sectors. Significant battles have been fought in the public sphere and have brought the discussion about civil rights versus security to the forefront. One exceptionally poignant example was illustrated in the San Bernardino, California terrorist attack. Two terrorists shot to death 14 people and wounded 22 others at the San Bernardino county department of health building.[48] The Federal Bureau of Investigation (FBI) sought a court order requiring Apple to provide the technical assistance they needed to gain access to one attacker's county-owned Apple iPhone 5c, but Apple's CEO, Tim Cook, did not cooperate citing customer privacy concerns.[49] Ultimately, the FBI gained access to the phone's data without assistance from Apple, but the public legal battle highlighted a conflict between two rights: public safety and security concerns versus individual privacy rights.

Privacy also has international implications. The U.S. views privacy differently from the European Union (EU), and these differences were exasperated when Edward J. Snowden disclosed a trove of classified information beginning in June of 2013. That summer, a British newspaper revealed that the NSA was collecting the telephone records of tens of millions of Americans, and had access to the servers of nine internet firms, including Google, Facebook, Yahoo, and Microsoft.[50] EU countries are sensitive to the transfer of their citizens' personal data abroad and enforce strict data localization rules on those responsible for its safekeeping. The Snowden disclosures brought the issue of individual privacy to the forefront and complicated diplomatic relations with the EU and others. As policymakers balance the needs of personal privacy versus public safety and security, the U.S. must act judiciously so as not to adversely affect international trade relationships.

Human Capital. The ICT industry faces significant challenges with regard to its requirements for a highly-skilled workforce. There are widespread shortages in the number of professionals entering the science, technology, engineering, and math (STEM) fields. These shortages can be attributed to three factors: (1) the relatively small number of domestic workers entering STEM fields; (2) constraints on immigration and the H-1B visa program; and (3) equality in the workforce, both for women and underrepresented minorities. By 2018, the U.S. Bureau of Labor Statistics estimates the total size of the STEM workforce at 8.65 million.[51] Yet, the U.S. struggles to produce enough students pursuing STEM careers, with some estimates predicting a shortfall of approximately one million U.S.-produced STEM professionals in the ten year period ending in 2022.[52] In 2014, the number of U.S. citizens and permanent residents earning graduate degrees in science and engineering fell five percent from its peak in 2008, while the number of students on temporary visas earning the same degrees soared by 35 percent.[53] Women and underrepresented minorities do not fill STEM jobs as frequently and women earn less. Women make up 48 percent of the U.S. workforce, but comprise just 24 percent of all STEM workers while earning 14 percent less on average.[54] African Americans, Hispanics, and Native Americans fare no better, representing only 11 percent of all engineering graduates.[55] Conversely, White and Asian workers make up 88 percent of all science and engineering jobs.[56]

Many ICT firms express the need for a diversity of ideas. Others emphasize the importance of a diverse workforce that represents its broad customer base. In all cases, it is clear the ICT industry requires a large and diverse STEM workforce to fill jobs and provide an expansive set of innovative ideas to foster a continuum of creative destruction in the industry.

Industry Outlook

Today, ICT has a central role in private and public sector markets. In regards to national security, the Department of Defense (DoD) relies heavily on U.S. high-tech companies to deliver a steady stream of sophisticated weapons systems. The 2015 National Security Strategy emphasizes the need to "grow investments in crucial capabilities like cyber; space; and intelligence, surveillance, and reconnaissance."[57] Also, the ICT industry is uniquely postured to safeguard and reinforce homeland security. The U.S. government in partnership with the ICT industry has made securing our Nation's critical cyberspace and physical infrastructure across every sector—financial, energy, transportation, health, and more—a top priority with the main objective of decreasing vulnerabilities and increasing resilience.[58]

The exponential growth in the ICT market and proliferation of the IoT has brought cybersecurity concerns to the forefront of the U.S. ICT industry. In contrast, the ICT IS saw less emphasis placed on cybersecurity within China's ICT industry. Nevertheless, cybersecurity appears broken from top to bottom, and if not properly addressed it will impede the industry's ability to achieve its full mobilization potential.[59] Bruce Schneier, a renowned cybersecurity expert, says "we are building a world-sized robot, in the shape of the Internet of Things."[60] Given the drive for the computerization of everything, Robert Watson, a computer scientist at the University of Cambridge says "the default assumption is that everything is vulnerable."[61] These vulnerabilities stem from the rapid pace of software development, online business growth, and economic growth of computer and software firms. Without slowing the pace of growth to address cybersecurity, the damage will be irreversible and the impact could be catastrophic. The good news is the industry leaders within the ICT industry are beginning to take notice and are taking corrective actions before the government has to step in.[62]

Short-term Industry Outlook (2017-2021). The growth of industrial activity in Silicon Valley has shifted the ICT ecosystem from its old vertical structure where one or two firms dominated the market to a horizontal structure where multiple companies are competing in different markets.[63] U.S.-based ICT conglomerates (Google, Facebook, Apple) appear to have a firm grip on their respective markets and will continue to dominate the global market in the short-term. However, globalization of the ICT industry will give rise to new ICT equipment makers and software challengers.[64] For example, China-based firms Lenovo, Huawei, Baidu, ZTE, and others are excelling in the global market and will threaten U.S. dominance across the entire ICT ecosystem from telecommunications, semiconductors, and wireless devices to computers.[65] According to a report published by the research consultancy International Data Corporation (IDC):

> the global information technology (IT) industry market, encompassing hardware, software, services, and telecommunications, is expected to reach $3.8 trillion in 2016, up from $3.7 trillion the previous year. The U.S. market accounts for approximately 28 percent of the total, or slightly more than $1 trillion. [However, o]ver the past decade, the biggest shift in global industry allocations stems from growth of the Asian region, fueled primarily by the rise of China.[66]

Long-term (2021-2035). In the long-term, the ICT industry will continue to focus on the computerization of everything in the form of IoT. Other technologies such as quantum computing (a possibly game-changing technology which would increase computing power exponentially), AI, virtual reality (VR), and machine learning will change the way we work and go about our daily lives.

The future advancements in AI and VR will make significant contributions in health care. VR technology will be used in diagnostics and robotic surgery (where surgery is performed by means of a robotic device—controlled by a human surgeon—which reduces time and risk of complications).[67] VR will also be used for training purposes and remote tele-surgery in which an operation is performed by the surgeon at a separate location to the patient.[68] In regards to AI, IBM's machine learning through Watson can understand all forms of data, interact naturally with people, and learn and reason, at scale. Collectively, AI and VR technologies will enable precise surgery in once complicated areas of the human body and make personalized treatment of patients achievable.

Political and Social Impacts. The next great wave of invention and economic disruption will be set off by continued advances in computing, advanced data analytics, and ICT. Advancements in technologies such as machine learning, advanced robotics, autonomous air and ground vehicles, the ubiquitous web and IoT promises to deliver a mixture of social stress and economic transformation.

Undoubtedly, these new technologies will bring vast improvements, as well as changes to our standards of living and overall welfare. However, some are concerned about the job-destroying power of the near and long-term technological wave. In 2013, Carl B. Frey and Michael Osborne, of Oxford University, examined how susceptible jobs are to computerization. They analyzed over 700 occupations and the expected impacts of future technology on the U.S. labor market and concluded that 47 percent of employment in the U.S. is at high risk of being replaced by automation within the next ten years.[69] Their model specifically predicts that most workers in transportation, logistics, and production occupations are at risk.[70] This is due in large part to advancements in computers that enable them to move beyond performing historically confined routine tasks involving explicit rule-based activities to performing pattern recognition and non-routine cognitive tasks.[71] In fact, China, which is known for its manufacturing capacity and low cost manpower, is investing heavily in automation manufacturing. For example, Chinese company Foxconn, a major supplier of Apple and Samsung products, has replaced nearly 60,000 factory workers with automation.[72]

Another concern with how rapidly technology is advancing is whether human workers can upgrade their skills fast enough to justify continued employment. In the past, new technologies boosted productivity with gains in revenue being split between skilled and less-skilled workers.[73] Now technology appears to be opening a great divide between the skilled, the wealthy few, and the rest of society.[74] In other words, the U.S. can no longer count on a growing industrial and manufacturing sector to absorb less-skilled workers. Consequently, our political system will struggle to accommodate the demands and growing numbers of dissatisfied workers.

The rapid pace of automation coupled with the divide between skilled and less-skilled laborers will test our political system. In many cases, government intervention and new regulations will attempt to slow the pace and overall job-destroying effects of ICT upon U.S. industries. The U.S. political system will likely struggle to accommodate the demands and growing numbers of dissatisfied workers. As a result, future political leaders sensitive to both sides of the debate will need to craft a plan that allows technology to benefit society and the economy more broadly.

Industry Position in the Global Marketplace. The U.S. ICT industry will continue to dominate the global marketplace for the foreseeable future. There are currently five undisputed tech giants of the U.S. ICT industry: Amazon, Google, Facebook, Apple, and Microsoft.[75] Financial reports and data indicate that these companies are getting larger, more entrenched, and more influential in new markets and sectors that startups might otherwise claim. For example,

these tech giants are making waves in healthcare and finance; they are building autonomous cars, unmanned aerial vehicles, and immersive virtual reality platforms that may change the way we communicate and view movies.[76] This is not to say these companies cannot be overtaken by ambitious startups or competition from abroad, but there remain significant barriers to entry.

However, a clear way for the U.S. ICT industry to ensure its continued global dominance is to be a disruptive innovator. The term "disruptive innovation" was coined by Clayton Christensen, in his book *The Innovator's Dilemma*.[77] Christenson makes the distinction between two different types of technology that affect business. First is what he called "sustaining technologies," which are less intensive developments that help companies make marginal improvements to existing products or processes.[78] Conversely, there are what Christensen regarded as disruptive technologies. He defined these technologies as "wild and unexpected technological breakthroughs that require corporations to radically rethink their very existence."[79] For example, the iPhone was disruptive when it was originally released in 2007. It changed the way we communicate by transforming a low functioning device into a mini portable computer used for voice, email and web browsing. Since that time, it has transitioned to a sustaining technology in a larger market of smartphones.

In summary, for the U.S. ICT industry to maintain its lead in the global market, it must choose between holding onto an existing market by doing the same thing better or capture new markets by embracing leap ahead technologies and adopting new business models.

Government Goals and Roles

President Obama "identified cybersecurity as one of the most serious economic and national security challenges" the U.S. faces and a challenge that the U.S. is "not adequately prepared to counter."[80] While the U.S. has implemented initiatives and policies, developed action plans, and stood up a military command (U.S. Cyber Command) to help provide security as well as economic and social benefit within this global cyberspace domain, the U.S. must still do more. The Nation needs to leverage all elements of its national power—diplomatic, informational, military, and economic—in order to prevent a devastating cyber attack on U.S. interests, ensure U.S. dominance within cyberspace, protect U.S. innovation and values, and foster the international digital economy, but it must delicately balance and prioritize U.S. Government roles within these efforts.

Since the Snowden disclosures, the international community and the American public continue to scrutinize U.S. security and regulatory efforts in cyberspace. These polarizing disclosures resulted in a general trend within the ICT Industry—highlighted by the much-publicized case of Apple's refusal of a U.S. Government order to unlock a San Bernardino attacker's iPhone—to balance more toward public privacy over national security; one European Union commissioner stated, "[m]utual trust and confidence have been seriously eroded and I expect the U.S. to do all that it can to restore them."[81]

In addition, the very nature of the U.S. Government—its size, complexity, bureaucracy, relative rigidity, and escalating budgetary constraints—limits its abilities to adroitly and broadly regulate in ICT-related matters, which are generally dynamic, volatile, and cascading in nature. This rigidity juxtaposed with the ICT Industry's agility, focus on innovation, and profit-seeking nature provides a very rich ecosystem for effective public-private partnerships. For all of these reasons, the U.S. Government should limit and prioritize its goals, roles, and oversight within the ICT Industry to only the areas required to maintain or enhance national security, help avoid or prevail over market failure, or directly support national interests. These efforts must focus

principally on close public-private partnerships followed by prescriptive regulation and policy-based solutions only when public-private partnerships prove impractical or ineffective.

Although the U.S. government should be cautious about regulating the ICT industry to prevent the potential effect of stifling innovation, it still has a role in terms of leveraging the elements of its national power to bolster U.S. national security, support U.S. interests, and minimize strategic vulnerabilities. Specifically, the U.S. should: (1) leverage diplomatic means, as well as close partnerships with industry and cyberspace experts (within the Intelligence Community, military, and academia) to collaborate with the international community (or independently, if required, due to the United States' power to influence global markets) to create enforceable cyberspace standards; (2) leverage diplomatic and military means to partner with international organizations—such as the North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defense Center of Excellence—to codify cyberspace behavior norms and treaties; (3) form a coalition of willing partners to self-police and ensure transparency (through robust information sharing) within cyberspace in order to ensure the common cyberspace defense of all parties; (4) reduce U.S. focus areas for critical infrastructure security to ensure effective prioritization while simultaneously reducing the overall attack surface by separating the infrastructures (to the maximum degree possible) from the internet; and (5) further educate the U.S. populace on cyberspace security while providing transparency on the role of government in cyberspace security. By heading down these proposed paths, the U.S. can reduce its vulnerabilities and increase its competitive advantage in cyberspace while improving public and international trust.

SELECTED ESSAYS ON MAJOR ISSUES

Cybersecurity and Digital Data by CAPT Stephen D. McKone

"Land was the raw material of the agricultural age. Iron ore was the raw material of the industrial age. Data is the raw material of the information age."

– Alec Ross, *The Industries of the Future*, 2016[82]

Digital data is now the most important global resource. The protection of all electronically stored data is the most important global security issue in the world today. This is not just the case for the DIB and the wider ICT industry, but for every individual, community, and nation worldwide.

The "Big Data Revolution."[83] "We now generate more data every two days than we did in aggregate from the dawn of early civilization through the beginning of the 21st century … and this information explosion accelerates each year by 40 percent."[84] The social media company Facebook has 1.86 billion members which equates to one out of every four people on earth. The company has personal data on 25 percent of the world's population stored in a data set that occupies 300 petabytes (PB) spread across nine global data centers.[85] The significant monetary value of this data to Facebook ($17.9 billion in revenues in 2016) demonstrates the criticality of cybersecurity in a world that continues to produce larger and larger amounts of invaluable data.

The Challenges of Cybersecurity. The protection of massive and exponentially growing digital data sets is the most significant challenge faced by cybersecurity practitioners today. The trend on the horizon will make the protection of data an even harder problem. Experts are monitoring the rapid expansion of global internet users and networked devices. By 2030, it is estimated that there will be 500 billion devices connected to the internet and an additional 5 billion

new internet users.[86] This expansion of cyberspace will increase the production of data to unimaginable levels while multiplying the attack surface for cyberspace attacks many times over.[87] Cybersecurity companies are currently monitoring over 1 million attempts per day to implant malicious software and virus signatures on customer systems.[88] It is difficult to fathom the number of daily attacks with an additional 5 billion users on the global network.

Evaluation of Private Sector Security Practices. Two troubling trends point directly to the current lack of effectiveness of cybersecurity in the private sector: (1) the rapid increase in data breaches, and (2) the widening gap between the time to compromise a system and the time to discover a data breach. The number of successful data breaches has exploded from several hundred in 2005 to over 2000 in 2015.[89] Verizon's data shows that the use of stolen login credentials is the most prevalent way systems are illegally accessed.[90] In 2016 alone, Shape Security detected over 3 billion sets of stolen login credentials.[91]

Therefore, the most cost effective and technically feasible method for companies to counter data theft is to block the use of stolen credentials by implementing multi-factor authentication (MFA). MFA requires either two or all three of the following pieces of information for system access: (1) something a user knows—like a password or personal identification number (PIN), (2) something a user has—like a cell phone or security token, and (3) who the user is—such as a piece of biometric data like a fingerprint or iris scan.[92] The almost universal ownership of smartphones in the U.S. combined with the widespread "bring your own device" (BYOD) culture in place across industry makes the implementation of MFA a very cost effective cybersecurity policy. The second factor can be delivered directly to an employee's personal mobile device (something the user has) via text message or by using an authentication code generating mobile application like Google Authenticator.[93]

The protection of data is arguably the most important national security and economic security task faced by the nation. Despite the predicted future growth of connected users and devices that make the future security of data seem like an impossibility, there are actions that can be taken today to protect this invaluable resource. The evolution of user credentials to multi-factor authentication systems will stem the tide of stolen data, lost value in the private sector, and unauthorized access to U.S. networks. At the federal government level the use of mandatory cybersecurity regulations is a national imperative to protect critical infrastructure and thus the economic security of the United States.

Critical Infrastructure by LTC Brady Stout

In their joint testimony before the U.S. Senate Armed Services Committee in January 2017, the Honorable James Clapper (Director of National Intelligence), the Honorable Marcel Lettre (Undersecretary of Defense for Intelligence), and Admiral Mike Rogers (Commander of U.S. Cyber Command and Director of the National Security Agency) highlighted that cyberspace threats have "challenged public trust and confidence in global institutions, governance and norms, while imposing costs on the global economy."[94] They also highlight that "[t]hese threats pose an increasing risk to public safety, as cyber technologies are integrated with critical infrastructure in key sectors."[95] The principal challenge the U.S. faces with regard to critical infrastructure security is that the "private sector owns and operates an estimated 85 percent of infrastructure and resources critical to … [the] Nation's physical and economic security."[96] Currently, the U.S. Government's approach—as defined in the 2013 Presidential Policy Directive on Critical Infrastructure Security and Resilience—is focused on private-public partnership and the application of security best

practices in which private sector participation is largely voluntary, government authorities are limited primarily to coordination and consultation, and transparency (due to the complexity of the intermeshing and interrelation of the infrastructures) is severely limited.[97] If the Congressional mandate is "that any … disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security,"[98] then the U.S. must update its laws and policies to provide proscriptive requirements to the companies operating critical infrastructures and directive authorities to the government agencies responsible for ensuring security and resilience within these infrastructures. Over the past fifteen years, the U.S. Government has instituted several laws and policies while granting roles to organizations within the Government to provide oversight to critical infrastructures, but the U.S. must still do more.

As several recent cyber attacks show, even highly protected and air-gapped systems (specifically, systems not directly connected to the internet and previously perceived as impenetrable) are vulnerable. These attacks include: the 2008 network intrusion by a foreign adversary into U.S. classified networks located in the Middle East;[99] the Stuxnet cyber attack from 2007 to its discovery in 2010, where Iran's adversaries sabotaged Iranian nuclear centrifuges in order to disrupt Iran's nuclear program;[100] and the 2015 and 2016 cyber attacks (purportedly conducted by Russian hackers in support of Russian military operations during the Russian military intervention in Ukraine) upon the Ukrainian power grid which each left over 225,000 Ukrainians without power for several hours.[101] If there is value—whether it be monetary, knowledge gained, costs imposed, or national security advantage gained—in exploiting a network, adversaries will work to find a way and will succeed given enough time, effort, and resources.[102] The heads of U.S. national intelligence support this position; they assert that "the cyber threat cannot be eliminated … [instead it] must be managed in the context of overall business and operational risk."[103]

The current critical infrastructure governance, oversight, and public-private partnership structure does provide some basic level of security, but does not provide a sufficient level of mission assurance which would effectively minimize "debilitating impact[s] on security, national economic security, national public health or safety, or any combination of those matters."[104] Much of the efforts surrounding critical infrastructure security—especially those measures focusing on cybersecurity—remain best effort levels of operation, focused toward (but not mandated upon) technology best practices, and reliant upon the owners' and operators' level of engagement, expertise, and support upon security. This leads to the dichotomy between the business trade-offs within these largely privately owned businesses and security efforts; in most cases, these security efforts do not provide standard business value or return on investment (ROI) to the owners and shareholders. In the case of cybersecurity within the energy grid, cybersecurity is not an area which would provide significant ROI considering that the majority of outages on an annual basis are due to animals; in fact, since 2013, animals have accounted for approximately 1,850 confirmed power outages around the world and human cyberspace operations have only accounted for two confirmed cases (both in the Ukraine).[105] Cybersecurity within critical infrastructure is largely a national security issue vice a business issue and should be treated as such. Cybersecurity should not be treated as a standard business practice within critical infrastructures managed as a routine part of standard business operations—especially since there is limited financial incentive for profit-seeking businesses to invest in it. To help improve cybersecurity within critical infrastructure, the U.S. must change its focus, update its laws, leverage industry expertise and advanced analytic capabilities, and optimize the whole of government approach based upon an analysis-based, prioritized, and risk-focused framework.

The U.S. can better secure its critical infrastructures and the Nation these infrastructures support by: (1) changing its focus on cybersecurity to be more proactive in nature; (2) Congressionally mandating information sharing to Department of Homeland Security (DHS) from private industry; (3) effectively partnering with private industry to leverage advanced industry artificial intelligence and machine learning capabilities to identify whole of system gaps and vulnerabilities; (4) harnessing this deeper understanding to more effectively prioritize investments and efforts to secure critical infrastructures; and (5) optimizing laws to better support governance and investment in critical infrastructure security. These efforts will help to balance conflicting priorities between infrastructure functionality, infrastructure business operations, shareholder investment, and security improvement as related to national security. As the 2003 U.S. power outage (the U.S.'s largest ever and due to overgrown trees and human error, which resulted in over 50 million people in the US and Canada living without power for up to two days, contributed to several deaths, and resulted in financial impacts up to $6 billion) shows, while cybersecurity remains a significant concern for critical infrastructure, the U.S. Government must also fully consider the environment and human activity when securing critical infrastructure.[106] By following the above recommendations and focusing efforts on the resulting prioritized gaps, the U.S. can effectively minimize the future impacts of failures and attacks upon critical infrastructures.

Big Data by COL Nicolas Tessaud, France

According to IBM, we create 2.5 quintillion bytes of data every day, and 90 percent of the data in the world today has been created in the past two years.[107] Big data analytics are unavoidable and have impacts on the whole society, from economic growth to government efficiency. The companies that embrace these analytics can hope to spur their growth, provided they set up informed strategies that best implement analytics use cases. Big data impacts national security on many levels. A senior logistics official noted that data is gold and every future contract should include a data policy. According to him, the DoD lacks a culture of data and is limited in the means to process it.[108]

Big data analytics can be defined as a way to store, query, and model large sets of information.[109] Any new big data project should start by analyzing five important "V" characteristics.[110] The first is the *volume* of the data itself. Then the *velocity* is used to characterize the streaming of data and the speed with which it has to be analyzed, sometimes in real time such as in the stock exchange trade information. Third, the *variety* describes the many different sources that have to be taken into account, from videos to tweets or IoT data. The *veracity* emphasizes that data has to be trusted and associated with a level of certainty to enable decisions. A fifth dimension is the *value* of big data, which describes the added value that must result from analysis.[111]

The worldwide market for big data analysis and services has been analyzed by a European Commission study. The market was expected to increase at an annual rate of 23 percent between 2014 and 2019. The forecast of global revenue is $187 billion in 2019, with more than half of it coming from the U.S.[112] The main U.S. market involved is business analytics and enterprise software publishing.[113] This industry develops and distributes business solutions to customer relationship management (CRM) and business intelligence (BI) based upon the analysis of data available. The revenue is estimated at $40 billion and is expected to grow at an annual rate of five percent through 2023.[114] The main companies operating in this market are Microsoft, SAP SE, Salesforce, Oracle and IBM.[115] The market share concentration and the competition are medium, as the four largest companies hold a share of 56.8 percent of the market.[116] Overall, this market can be labeled as a monopolistic competition.

Even if the use of big data analytics is a global trend that every company should consider, it is not so simple and it has to be a case-by-case decision. Businesses can waste a lot of energy if they have not prepared and focused their use cases for data analytics, and successful big data transformations begin with the assessment of the value drivers and capabilities in comparison to the competition.[117] There are also issues to be addressed. An important one is ethics, as analytics could lead to discrimination or others' misuse by overgeneralization of statistics.[118] Another issue is the lack of human capital. A 2016 study reported that the U.S. faces a shortage of up to 190,000 people with deep analytical skills and 1.5 million managers and analysts to process big data in order to make informed decisions.[119]

This technology is in full development, and companies in Silicon Valley are dynamically innovating in this promising trade-space. The trend today is to go toward on-the-fly analysis, thus lowering the need of extensive data storage facilities. The next step will be to combine big data and the IoT. The explosion of the number of IoT devices—50 billion by 2020, as previously discussed—ensures that the global amount of data will continue to grow and probably more than double every two years.[120] A 2016 survey showed that 44 percent of companies aim to use IoT in their strategy, and they cannot do that without assessing the best means and business value of analyzing the volume of data produced by these devices.[121] Finally, future technology development may prove to be the enabler of even greater analytic potential. The two main technologies identified are quantum computing, that promises to be the next leap in processing speed, and cognitive computing developments such as IBM's Watson technology that will enable machine learning and easier queries among larger data sets.[122]

The overall impact of big data on economies is linked with the best practices of each particular sector. Overall, companies can hope to gain up to ten percent productivity growth by using data analysis with respect to the ones that do not.[123] An analysis conducted by the European Commission reported a potential growth of 1.9 percent of EU's GDP between 2014 and 2020 thanks to big data analytics.[124] A direct impact of analytics has been reported in the gaming industry by a Californian company, with the ability to analyze the behavior of the players and then target them with a personalized experience, thus addicting them and gaining sustained growth for the company. In addition, a research institute in Hong Kong reported that by using targeted marketing campaigns for banking products, banks had doubled the return ratio.

Governments can use big data analysis as well. The main applications would be to enhance operational efficiency, transparency, citizen's wellbeing and engagement in public affairs, economic growth and national security.[125] However, an extreme use of big data analytics can be observed in China, where the government is setting up a "Social Credit" database to assess the faithfulness of Chinese people.[126] This system is discussed in detail in the privacy section of this document. The main challenge of big data within the government is the collection of data, as it comes from many different channels and under different formats. Overall, the potential impact of the full use of data analytics in the 23 largest European governments could reduce administrative costs by 15 to 20 percent.[127] The main drivers are a greater efficiency, an increased tax collection rate, and a reduction of fraud and errors.[128]

Big data is foreseen to have a positive impact on national security in many ways; it will help government operations related to countering international terrorism, law enforcement, countering insider threats, critical infrastructure protection, military operations, and cybercrime.[129] The main drawbacks are a greater attack surface to potential cyberattacks, and a surrendering of a part of sovereignty.

In order to spur the growth of big data analytics, the U.S. and allied nations should implement four policies. First, they should establish analytics agencies to provide oversight on the

different big data approaches and to facilitate the integration of the many different data sets in order to further innovate analysis.[130] Second, in order to address the privacy requirement, each nation must set clear regulations regarding personal data protection, by extending and facilitating the use of anonymized data. Third, data ownership is a complex topic, as big sets of data usually have multiple sources and owners.[131] Thus, the rules for selling and buying data have to be more formalized in order to prevent abuse of dominant positions and to ensure efficient, effective, and lawful uses of data. Lastly, the requirements coming from data localization policies can decrease the availability of data sets, and specific regulations should be devised to allow the processing of data without localizing it, with on-the-fly analysis, for example.

Big data analytics is a flourishing market, but the future potential impact of this technology is tremendous, whether in the overall economy, in governmental use, or in the national security field. For DoD, big data could very well be an essential element of its third offset strategy. The main concerns are cybersecurity, sovereignty, and privacy; the four policies proposed above will help address these concerns. The next challenge is to go even further and harmonize the use of data across nations by building trust and ensuring the respect of each country's sensitivity to privacy.

Privacy: Domestic and International by Lt Col Tony England and COL James Walsh

The world's population is using ICT to interact through social media, make international investments, and spread valuable information that is collected and stored in huge volumes, both domestically and internationally. Much of the data is personal information and many people are blissfully unaware that governments and corporations are gathering it for surveillance and tailored marketing efforts. In many instances, people are unable to individually protect their information due to laws, policies, and business practices. As a result, protecting individual privacy rights is a significant concern across the globe; it is all the more so because of the conflicting frameworks employed in key regions. This essay discusses three key frameworks that are shaping the current global discussion.

The United States. The U.S. has long promoted the idea of individual privacy. The Fourth Amendment to the *U.S. Bill of Rights* protects Americans against unreasonable searches and seizures while the Fifth Amendment ensures the "privilege against self-incrimination, which provides protection for the privacy of personal information."[132] In his famous dissenting opinion in the 1927 Supreme Court case *Olmstead v. United States*, Justice Louis Brandeis wrote that the Founding Fathers "conferred against the government, the right to be let alone—the most comprehensive of rights and the right most favored by civilized men."[133] Nevertheless, the U.S. still strives to effectively balance the role of electronic surveillance with individual privacy and security.

In the aftermath of the 1972 Watergate scandal, the U.S. Senate's Church Commission discovered broad Executive Branch-directed government surveillance of American citizens. In response, Congress passed the *U.S. Privacy Act of 1974*, which, though subsequently modified, defines America's surveillance framework. Additionally, Congress passed the 1978 *Foreign Intelligence Surveillance Act* (FISA) that established the FISA court which oversees government electronic surveillance requests for foreign spies and agents of foreign powers operating inside the U.S. In 2013, National Security Agency contractor, Edward Snowden, revealed an American surveillance program capable of gathering data from virtually every nation on Earth.

As a result of Snowden's disclosures, the U.S. passed the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online

Monitoring (USA FREEDOM) Act in 2015.[134] The Act reversed the bulk collection programs that had created domestic civil rights concerns and international diplomatic turmoil resulting from Snowden's disclosures. The new rules require the government to obtain a court order before requesting specific segments of information from domestic telecommunication providers. Importantly, the Act increased transparency by enabling companies to report information on FISA orders and by requiring a declassification review for some FISA orders. While incidental collection of U.S. citizens continues to be a challenge, the new Act has made significant improvements in striking a balance between security and privacy.[135]

The European Union. "Cross-border data flows between the U.S. and Europe are the highest in the world, almost double the data flows between the U.S. and Latin America and 50 percent higher than data flows between the U.S. and Asia."[136] Although both agree that individuals should have privacy rights, the U.S. and EU do not share the same privacy policies or take the same approach in protecting personal data. A primary difference between the U.S. and Europe is that the U.S. allows collecting and sharing personal data unless there is "a law prohibiting" the collection while the EU prohibits processing personal data unless there is "a law allowing" the collection.[137]

In 1995, the EU developed a "Data Protection Directive" prohibiting the transfer of personal data to non-EU countries unless those countries could first meet the standards for privacy protection. Assisting 3,000 companies in complying, the U.S. worked with the EU to develop a shared framework called the "Safe Harbor Privacy Principles."[138] However, the agreement was put in jeopardy after the Snowden disclosures and when the U.S. Center for Digital Democracy filed a complaint against 30 U.S. companies that had collected private data on EU residents, "including online tracking, purchasing history, addresses, income and family structures."[139] As a result, in 2016, the EU-U.S. "Privacy Shield" agreement was created. The agreement provides the EU with assurances that "any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms."[140] In addition, the *U.S. Judicial Redress Act of 2016* extended the rights afforded in the U.S.'s 1974 *Privacy Act* to EU citizens and allowed the use of U.S. courts to enforce privacy rights issues.[141]

Furthermore, the EU decided that search engine companies must honor requests from its users to delete links to personal information. The action, termed "The Right to Be Forgotten," provided individuals a way to erase irrelevant information that no longer applied.[142] In 2018, the EU's new "General Data Protection Regulation" will further extend individual rights by forcing companies to delete all requested personal data. It applies fines up to 4 percent of a company's revenue for privacy rule breaches. For Google, this could mean billions of dollars in fines.[143]

People's Republic of China (PRC). For the second straight year, the Freedom House Internet-freedom rankings placed China last in the world based largely on government crackdowns on free expression.[144] Chinese law makes it illegal to spread rumors via social media with *Global Voices* reporting that Chinese nationals could be arrested "if their posts are viewed 5,000 times or forwarded 500 times."[145] As internet use continues to expand in China, the government maintains the ability to isolate the nation from the global internet through the nine state-run internet gateways. Earlier this year, China's internet censorship efforts, commonly known as the Great Firewall, took another major step when the government announced a 14-month effort to "clean up" internet access including stopping the use of unregistered virtual private networks which allow internet users in China to bypass government monitoring.

As big data analytic efforts spread, China is employing the technology to enable societal control through a "social-credit system." The system, which began limited testing in 2016,

accesses digital information to monitor, among other factors, internet usage. While such data collection is not new, especially with companies such as Facebook and Google maintaining troves of user data, China's personal privacy laws differ greatly from those in Europe and America. For example, China created laws in 2016 expanding real-name and personal information registration requirements for websites and service providers.[146] Given the potential negative impacts, it is not surprising that the Freedom House reports that digital activism and social discussion have declined in China.[147]

The internet provides connections for social media, global trade, financial transactions, and other information sharing capabilities. However, with connectivity comes responsibility in governing how data is stored, how it's collected, who has jurisdiction, and how to protect individual privacy rights. The U.S. should continue to lead in promoting information sharing while creating individual privacy policies that satisfy not only the EU, but the entire international community.

Information and Communications Technology Acquisition
by Lt Col Rodney Stevens and Ms. Sheila Harris

One of the largest issues concerning U.S. government interaction with the ICT industry—an industry defined by rapidly changing technologies, and constant fluctuations in market competitors—is with regard to how the DoD conducts ICT acquisition. The DoD recognized the need to reach out to ICT firms it has not historically done business with in the past to ensure dominant capabilities are delivered on cost and on schedule. In April 2015, the DoD codified this recognition in Better Buying Power (BBP) 3.0, the guiding concept by which the DoD can achieve these dominant capabilities through technical excellence, innovation, and effective partnership with industry. To help achieve these goals, the DoD is reexamining business arrangements, so it can: (1) attract and enable a broader array of industry participants; (2) employ techniques that will motivate industry to deliver tangible results that advance combat capabilities; and (3) recognize that deliberate speed is required to stay ahead and remain on the cutting-edge.

Regrettably, several DoD Major Automated Information System (MAIS) acquisitions which are within the ICT domain have experienced numerous schedule delays and cost overruns. In 2016, the DoD spent approximately $2.5 billion on its MAIS investment portfolio spanning a wide range of IT system types.[148] Currently, there are 35 designated MAIS programs of which 18 were assessed by the General Accountability Office (GAO) in 2016. Of those programs assessed, 62 percent have experienced cost increases on average of $457.2 million, with 78 percent of the programs having scheduled delays ranging from 2 months to 13 years.[149] Many believe a considerable amount of these shortfalls can be attributed to the DoD's constrained procurement process which has been institutionalized in a bureaucratic system that is embraced by an antiquated, risk averse program office culture overseeing such programs.[150]

Recognizing commercial industries have surpassed defense programs at innovation and speed of delivery, in late 2015 former Secretary of Defense (SECDEF) Ashton Carter directed the DoD to establish new relationships with private sector companies principally located in Silicon Valley, and with other companies located in the technology focused hubs of Boston and Austin, to address the problem. The venture known as Defense Innovation Unit Experimental's (DIUx) main objective, on a comparatively smaller scale than most DoD acquisition programs, has been to tap into the "tech startup" sector and its culture to meet national security mission needs. Knowing that the Silicon Valley tech startup culture has created such successes as FireEye cybersecurity, the social media giant Facebook, and the internet search engine goliath Google, the

question becomes, "why limit the DIUx approach on a small scale within DoD acquisitions?" Granted, many recognize there are several instances where the DIUx model is not practical for acquisition programs. Nonetheless, there may be an opportunity for the DoD to develop programs within the ICT industry following this framework.

A former Google employee, Isaac Taylor, characterizes the issue with the DoD process best, "[i]n Silicon Valley's culture, meetings end either with a decision, a deal or whether a deal is possible. In the Pentagon's culture, meetings lead to more meetings, which might lead to a [research and development] contract in 18 months, followed by testing, approval, then renewed competition to build a prototype, then an assessment followed by several more stages."[151] From the beginning, Secretary Carter charged the DIUx to access cutting-edge technology from "non-traditional DoD" vendors, change the way the DoD has done business in the past, and adapt commercial best practices to lower its barriers to entry and transform into a more attractive customer. In response to his decree, DIUx initiated a first-of-its-kind acquisition mechanism known as the Commercial Solutions Opening (CSO) which is aimed to be fast, flexible, and collaborative. Under this approach, DIUx solicits capability solutions to problems that the warfighters are facing by awarding prototype projects, known as Other Transactions (OT)—an agreement unlike contracts that is ***not*** bound by the Federal Acquisition Regulation (FAR).[152]

As a matter of law, Title 10 U.S.C 2371, Section 815 affords DIUx the authority to pursue authorities for prototype development outside of the FAR process when costs are less than $250 million. One of the greatest advantages to the DIUx approach is the ability to award contracts quickly and the opportunity to enter cost-sharing arrangements with vendors. While Title 10 U.S.C 2371 specifies that competition should be pursued to the maximum extent possible, under the OT authority DIUx utilizes the mandates outlined by the Competition in Contracting Act (CICA) do not apply. This affords DIUx flexibility in prescribing competitive procedures to meet their objectives and mission needs in a timely manner. As for funding, cost-sharing is required for traditional defense contractors, whereas nontraditional contractors can either enter a cost-sharing arrangement or in-kind contributions toward the development of the prototype system. Like the CICA exceptions, under the OT authority DIUx does not have to enforce the onerous government cost accounting standards required by traditional acquisitions. Lastly, one of the most beneficial characteristics of the DIUx OT approach is the ability to quickly move from prototype to production. The 2016 National Defense Authorization Act (NDAA) granted the authority to DIUx to award follow-on production contracts or transactions without re-competing the work, provided the original OT was competitively awarded and that the prototype project was successful.[153]

The innovative acquisition model DIUx utilizes appears to be an approach which could benefit major DoD MAIS programs. As previously noted, many of those programs across all branches have struggled to meet cost and schedule objectives. Nevertheless, DIUx is still a relatively new organization and the authorities it has been afforded have been in place for just over a year. The administrative results are still promising; in June 2016, when DIUx instituted its new business practice, it awarded twelve Other Transaction (OT) contracts with the average award taking a mere 59 days. There are those who have their doubts, however. During the ICT IS's visit to Silicon Valley, a former Senior Defense official shed doubt on the DIUx initiative, expressing he felt it was not meeting its intended objective set out by SECDEF Carter, and sensed the DoD was better served to pursue such DIUx prototype efforts through DARPA.[154] However, DARPA is strictly a research and development caldron. In order for DARPA development projects to pass into production, they would have to be turned over to a military service to pursue through the traditional acquisition process unless Congress changes DARPA's authorities.[155]

In November 2016, the former Undersecretary of Defense for Acquisition, Technology, and Logistics (USD/AT&L), Mr. Frank Kendall, sent an "all hands" email touting the OT methodology while praising DIUx for employing OTs to rapidly meet warfighter requirements.[156] His email was not a memo or a directive though. DIUx, despite its infancy and doubters, does offer an approach which should be considered for MAIS acquisitions programs within the ICT industry. In additional to the DoD's BBP 3.0 initiative, there appears to be an opportunity for USD/AT&L to codify and cross-pollinate the DIUx mantra through similar BBP directives to the military services in an effort for them to improve their acquisition communities' development and delivery of MAIS systems within the ICT industry.

Human Capital by Ms. Kelli Lozada-Reese

If one has ever watched the movie, Jerry Maguire, then one knows the phrase, "show me the money."[157] A sports representative spends his days soul searching and in pursuit of procuring a free agent football player a big paycheck, spending his time focused on the quality of his client rather than on the quantity.[158] Yet what the characters find out is that human aspects are critical. They become friends, collaborate, give back, learn, and ultimately, humility brings them the good fortune of the money they were seeking.

These themes were present across the ICT industry and throughout our field studies visits. From the garage startups to the big buildings, the paycheck, no doubt a driver, was not the focus of the companies that are showing the most gains in human capital recruiting and retention. What was apparent is the competition is not about innovation. The competition is about the journey to innovation. The core of the ICT human capital model, primarily during the domestic field study and to a lesser extent in the PRC was about the benefits for the people.

Human capital, according to the Oxford Dictionary, is defined as "the skills, knowledge and experience of a person or group of people, seen as something valuable that an organization or country can make use of."[159] What the ICT IS came to realize through its studies, is that ultimately all definitions lead to the worth of an employee. That value comes from an investment in the person, their education and training, and their potential to earn money or add value to an organization. Not until the last fifty years did gender, diversity, and generational challenges take on a more substantial role in the workplace. So, as these roles expanded in the workplace, so did the challenges. Human capital has become a new work unit, widely expanded to include insurance, sick leave, exercise benefits, maternity leave, and training within organizations.[160]

The ICT industry is very forward thinking and generally deeply cares about its people. One company pointed out, "employees are no longer only interested in themselves in the workplace, but about the footprint they are leaving with those around them. They want to work for a distinct mission and along the way give back."[161] Several companies such as Shape, Cisco, Facebook, Google, and FireEye spend a good deal of time giving back to the community, whether it is judging a high school STEM science fair, donating food to the needy, mentoring, or even woodworking, giving back is now a new currency.[162] No doubt that self-awareness breeds humility.

Therefore, if there is so much right with the industry, what could be wrong? The lack of women, diversity, and mixed generations has continued to be a challenge for the ICT industry. These are all known issues to the industry and many companies are addressing the concerns, some effectively while others more slowly.

There is a lack of employees in America with the right STEM skill sets to fulfill many ICT industry roles. Therefore, the industry uses the immigration and H-1B Visa programs to bring in employees from other countries to serve in many STEM roles. With uncertainties about

immigration reform and the continued desire to hire U.S. citizens, the industry needs to support STEM programs across the country to increase the number of qualified and well-compensated graduates. With women and minorities trailing in the field, the industry needs to be aware of these concerns and take additional action to improve.

Diversity in the workplace matters according to multiple reports, where companies with diverse workforces have consistently increased their financial gains.[163] In the competitive landscape and globalized marketplace, this makes a lot of sense and should be embraced by all employers, especially those in the ICT industry who create technology for the world.[164] Diversity brings different backgrounds that can prepare better, promote broader thought, and improve overall decision making.[165] Diversity programs are taking on new meaning in the industry and are gaining momentum toward employing more diverse workforces in the coming years.

Women are important to the industry and have made vital contributions over time, yet they make up a small percentage of STEM workers in the ICT industry. This brings to light the importance of gender and cultural norms for women and ensuring from a young age that women are pushed towards all career fields, not just what will offer the most flexible career. Many of the most competitive firms in Silicon Valley offer benefits to men and women equally in the workplace, and will find ways to assist anyone who has the right skills. For the ICT industry, it does not matter who created the innovation, so long as it was created. To address the lack of women in the field, the ICT industry is involved with programs such as Girls Who Code, which hopes "to close the gender gap in technology."[166] Without actively working towards closing the gender gap with larger financial contributions, some organizations may continue the downward spiral.[167]

With Baby Boomers, Gen Xers, and Millennials comes a subset of characteristics and stereotypes. There is a new term, Gen Z, that suggests the workplace should stop focusing on supporting each of the generations in the same manner as the past. Instead, focus on their "hyperconnected" behaviors and how to best meld them together so the workforce is more cohesive.[168] The focus, as the IS learned in Silicon Valley, and with much of the ICT industry, is on the individual's experience; this is the primary concern moving forward. Companies are embracing this concept and ensuring that the mission is as important, if not more so, than the monetary benefit. This is a paradigm shift where the human capital strategic messaging teams are using multiple outlets to capture the spirit of their employees. Work today, for many is the freedom to ride their bikes to work, socialize with their comrades in the arcade, have healthy lunches in company cafeterias and restaurants, maintain flexible work schedules and work locations, and build lifestyles around their work.

The ICT industry, for many years, has been an industry on the cutting edge of many revolutions. Not surprisingly, they are also ahead of the federal government in how they approach human capital in their culture and work environments, not in evolutionary increments but with revolutionary changes. Innovation is deep at the core of the profession. No matter your gender, diversity affiliation, or age category, there is something for everyone in the ICT industry. With perks such as cappuccino, Magnum ice cream bars, sushi, bike racks, arcades, and yoga rooms, there are companies that are interested in not only gaining an employee, but impacting a lifestyle and culture. They know that to compete with others in the ICT industry, they have to be more than an average high tech company. Many of these companies possess fearless leaders that have a hope in something larger than themselves and ultimately in more than "show me the money."

Conclusion

The ICT industry is extremely broad and spans from consumer gadgets, to corporate IT services (such as cloud computing, data processing and analytics, and cybersecurity services), telecommunications services, to the unrealized potential of AI, VR, and quantum computing. The current state of the industry remains healthy with continued prospects for growth as the digital economy continues to expand. The U.S. remains the global leader in the ICT industry with U.S. technology giants in the top-five spots: (1) Amazon, (2) Google, (3) Facebook, (4) Apple, and (5) Microsoft.[169] However, globalization is giving rise to new challengers in the ICT industry—such as Lenovo, Huawei, Baidu, ZTE, and others—that are gaining global market share and threatening U.S. dominance in current technologies. To counter, the U.S. must leverage its global leadership in innovation to mature the technologies of the future—such as quantum computing, AI, VR, and machine learning—to maintain its lead in the ICT industry.

The U.S. ICT industry faces a number of other challenges, as well. The industry's drive for profits coupled with consumers generally preferring ease of use over security often leave cybersecurity in consumer products as an afterthought. As cyberspace threats become increasingly sophisticated—amongst a general public that is only now starting to realize the dangers within cyberspace—the ICT industry must become much more proactive in incorporating cybersecurity into their products and not wait for a catastrophic event before taking action. Digital privacy is also a growing concern of not only individual consumers, but also of foreign governments, especially after the Edward J. Snowden disclosures. These privacy concerns are driving foreign governments to consider policies—such as data localization requirements—that inhibit digital trade. Lastly, the U.S. has a shortage of professionals entering the STEM fields. Professionals in STEM fields are the catalysts for innovation that drive the ICT industry forward and create new business opportunities.

Despite the many challenges facing the U.S. ICT industry, the government should exercise restraint (despite pressures to do otherwise) on its oversight within the ICT industry and narrow its policy focus primarily to issues impacting national security, market failure, or specific national interests. The U.S. government should leverage public-private partnerships, domestically and internationally, to pursue partnered solutions before establishing prescriptive laws and regulations that are unable to keep pace with the ICT industry and potentially stifle the rapid pace of innovation that enables the U.S to remain the global leader in ICT.

Appendix 1

Category	NAICS	Title	Industry Defination	Firms
IT Hardware				
	33421	Telecommunication Networking Equipment Manufacturing in the U.S.	Manufactures wired (voice and data) telecommunications equipment, including telephone switching systems, telephones and answering machines, data bridges, routers, modems and gateways	Cisco Systems Inc.
	33422	Communication Equipment Manufacturing in the U.S.	Primarily manufactures broadcasting and other wireless communication equipment.	Harris Corporation, Cisco Systems Inc.
	33411a	Computer Manufacturing in the U.S.	Manufacture and assemble personal computers, laptops and servers. Operators typically purchase computer components (e.g. motherboards and graphics cards) from dedicated manufacturers in other industries.	Hewlett-Packard Inc., Dell Inc., International Business Machines Corp.
	33411b	Computer Peripheral Manufacturing in the U.S.	Manufacture peripheral equipment for computers such as monitors, keyboards, mice, printers, scanners and terminals.	Hewlett-Packard Inc., Western Digital Corp., Seagate Technology
	33441a	Semiconductor and Circuit Manufacturing in the U.S.	Manufacture semiconductors and related devices and parts. Products include integrated circuits, memory chips, microprocessors, diodes, transistors and other optoelectronic devices.	Samsung, Intel Corp.
	33441b	Circuit Board and Electronic Component Manufacturing in the U.S.	Manufacture electronic components (except semiconductors and devices), such as printed circuits, circuit boards, capacitors, transformers, connectors and switches.	TE Connectivity
IT Services				
	54151	IT Consulting in the US	Includes firms that provide the following services to client companies: writing, testing and supporting custom software; planning and designing integrated hardware, software and communication infrastructure; and on-site management of computer systems and data processing facilities. This industry excludes packaged software publishers and off-site data processing and hosting services.	International Business Machines Corp.
	51821	Data Processing and Hosting Services in the U.S.	Data processing services provide specialized reports from information supplied by clients. Hosting services can include web and application hosting. Services range from automated data entry to processing data.	Hewlett-Packard Inc., Dell Inc., International Business Machines Corp.
	51913a	Search engines in the U.S.	Firms operate search engines and search-based websites that display advertisements. The engines are typically free to use and earn income when a user follows and advertising link known as a "paid click."	Alphabet Inc., Microsoft Corp.
	51913b	Internet Publishing and Broadcasting in the U.S.	Firms offer nonphysical products such as news, music and video exclusively thorough the internet. Revenus is derived from the sale of advertising space or subscription to consumers.	Alphabet Inc., Netflix, Inc., Facebook

Appendix 1 (continued)

Category	NAICS	Title	Industry Defination	Firms
Software				
	51121	Software Publishing in the U.S.	Publishers disseminate licenses to customers for the right to execute software on their own computers. Operators market and distribute software products and may also design the software, produce support materials and provide support services.	Microsoft Corp., International Business Machines Corp., Oracle
	51121a	Operating Systems & Productivity Software Publishing in the US	Firms develop and publish operating systsms and productivity software. Firms also generate revenue from tech support and software resales.	Microsoft Corp., Apple
	OD5392	Software Testing Services	Provides software testing services for clients, such as performance testing, stability testing, usability testing and security testing. This industry does not sell its own software, but it may use internally developed software to complete its testing tasks.	There are no major firms in this industry.
	OD4816	e-Discovery Software Publishing	Any process through which electronic data is searched, located and secured for use as evidence in a court of law	Hewlett-Packard Enterprise Company, FTI Consulting, Inc.
Telecom Services				
	51721	Wireless Telecommunications Carriers in the U.S.	Firms operate and maintain switching and transmission facilities to provide direct communication through radio-based cellular networks.	AT&T, Verizon Communications, Deutsche Telecom, Sprint
	51711c	Wired Telecommunications Carriers in the U.S.	Provides local and long distance voice communication services using the public switched telephone network. Industry operators also generate revenue by providing internet access and video services and by wholesaling access to their networks. This industry excludes operators that solely resell telecommunications services.	AT&T, Verizon Communications, CenturyLink
	51711e	voice over internet protocol (VoIP)	Provides VoIP services to consumers, businesses and government organizations. VoIP technology converts voice signals into digital data that is transmitted using the internet. This industry does not include VoIP providers who bundle their services with internet, cable operated VoIP, and operators that resell VoIP services.	Vonage Holdings
	51791a	Telecommunications Resellers in the U.S.	Firms purchase access and network capacity from operators of TELECOM networks and resell these services to businesses and households	America Movil SAB de CV
	51741	Satellite Telecommunications Providers in the U.S.	Firms provide connections via satellite for broadcasters and other TELECOM providers. Includes resellers of satellite TELECOM services but excludes direct-to-home satellite TV services.	Intelsat Ltd., EchoStar Corp.

ENDNOTES

[1] Rachel Fefer, Shayerah Ilias Akhtar, and Wayne Morrison, "Digital Trade and U.S. Trade Policy," *Congressional Research Service: Report*, January 13, 2017, 1–43, https://nduezproxy.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=120924298&site=eds-live&scope=site.

[2] Department of Defense, DoD Dictionary of Military and Associated Terms, (Washington, DC: Joint Chiefs of Staff, March, 2017), 60, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed April 17, 2017); the Department of Defense defines cyberspace as "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."

[3] Barack H. Obama, "National Security Strategy" (Washington, D.C., 2015), https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

[4] "IT Industry Outlook 2017," CompTIA Information Technology, January 2017: p. 6, accessed April 12, 2017, https://www.comptia.org/resources/it-industry-trends-analysis-2017; IBISWorld, "U.S. Industry Market Research and Industry Risk Ratings Reports," *Ibisword.com.* http://clients1.ibisworld.com/reports/us/industry/home.aspx.

[5] "IT Industry Outlook 2017," CompTIA Information Technology. January 2017. p. 6. Accessed April 10, 2017. https://www.comptia.org/resources/it-industry-trends-analysis-2017.

[6] Stephanie Overby, "The top 10 IT outsourcing service providers of the year," CIO, February 08, 2016, accessed April 14, 2017, http://www.cio.com/article/3030989/outsourcing/the-top-10-it-outsourcing-service-providers-of-the-year.html.

[7] IBISWorld, "U.S. Industry Market Research and Industry Risk Ratings Reports," *Ibisword.com.* http://clients1.ibisworld.com/reports/us/industry/home.aspx, accessed April 9, 2017.

[8] Ibid.

[9] "47 U.S. Code § 153 – Definitions," Cornell University Legal Information Institute, accessed April 13, 2017, https://www.law.cornell.edu/uscode/text/47/153#50.

[10] IBISWorld, "U.S. Industry Market Research and Industry Risk Ratings Reports," *Ibisword.com.* http://clients1.ibisworld.com/reports/us/industry/home.aspx.

[11] Soumitra Dutta, Thierry Geiger, and Bruno Lanvin, "The Global Information Technology Report 2015," *World Economic Forum.* http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf, p. xv, (Accessed April 8, 2017).

[12] Ibid, p. xv.

[13] Ibid.

[14] Rachael King, "Dell posts strong PC sales, but servers slump." *Marketwatch.com,* December 8, 2016. http://www.marketwatch.com/story/dell-posts-strong-pc-sales-but-servers-slump-2016-12-08. (Accessed April 8, 2017).

[15] Ibid.

[16] Ibid.

[17] Davis Linthicum, “The cloud is killing traditional hardware and software,” April 23, 2013, accessed April 8, 2017, http://www.infoworld.com/article/2614536/cloud-computing/the-cloud-is-killing-traditional-hardware-and-software.html April 8, 2017.

[18] Ibid.

[19] Department of Defense, DoD Dictionary of Military and Associated Terms, (Washington, DC: Joint Chiefs of Staff, March, 2017), 60, accessed May 4, 2017, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf; the Department of Defense defines cybersecurity as efforts taken to prevent damage to, protect, and restore “computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”; Billy Mitchell, “Federal cyber-incidents were down in 2016 — at least on paper,” Fedscoop.com, February 14, 2017, https://www.fedscoop.com/federal-cyber-incidents-2016-least-paper/.

[20] Steve Morgan, “Hackerpocalypse: A Cybercrime Revelation,” Cyber Security Ventures, accessed May 4, 2017, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[21] IBISWorld, https://www.clients1.ibisworld.com/reports/gl/industry/industryoutlook.aspx

[22] Ibid.

[23] Ibid.

[24] Eric Griffith, “What is Cloud Computing?” PCMag.com, May 3, 2016, http://www.pcmag.com/article2/0,2817,2372163,00.asp (Accessed March 18, 2017).

[25] National Institute of Standards and Technology, “Final Version of NIST Cloud Computing Definition Published.” NIST.com, September 16, 2016, accessed March 21, 2017, https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published.

[26] Ibid.

[27] Ibid.

[28] Statistical Analysis System (SAS) Institute, “Big Data: What it is and why it matters,” *SAS.com*. 2017, accessed April 9, 2017, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.

[29] Ibid.

[30] Ibid.

[31] Jessica Davis, “Big Data Goes Mainstream: What Now?” *Informationweek.com*, January 14, 2016, accessed April 9, 2017, http://www.informationweek.com/big-data/big-data-analytics/big-data-goes-mainstream-what-now/d/d-id/1323874.

[32] Ibid.

[33] Christina Erbe, "Internet Publishing, Broadcasting and Search," The University of Iowa, February 10, 2015, accessed May 11, 2017, http://tippie.biz.uiowa.edu/henry/reports15/Internet.pdf.

[34] Ibid.

[35] Ibid.

[36] Internet Society, *The Future is Forever IPv6*, http://www.worldipv6launch.org/infographic/

[37] Cisco Internet of Things, "Learning about the Internet of Things", *Cisco.com*. accessed April 9, 2017, http://www.cisco.com/c/r/en/us/internet-of-everything-ioe/internet-of-things-iot/index.html.

[38] "Security risks from the internet of things," *TechTarget.com*, accessed May 11, 2017, http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Security-risks-from-the-internet-of-things.

[39] IBISWorld, https://www.clients1.ibisworld.com/reports/gl/industry/industryoutlook.aspx

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Connections, "IDC forecasts global ICT spending to reach US$3.5 trillion this year", *Connectionsplus.ca*, March 7, 2017, http://www.connectionsplus.ca/idc-forecasts-global-ict-spending-reach-us3-5-trillion-year/1002879266/

[44] IBISWorld, https://www.clients1.ibisworld.com/reports/gl/industry/industryoutlook.aspx

[45] Internet Society, *The Future is Forever.*

[46] Nancy A. Renfroe and Joseph L. Smith, "Threat / Vulnerability and Risk Analysis," Whole Building Designer Guide, last modified August 8, 2016, accessed May 6, 2016, https://www.wbdg.org/resources/threat-vulnerability-assessments-and-risk-analysis.

[47] "2017 Credential Spill Report: Key Findings," *Shape Security*, accessed April 20, 2017, http://info.shapesecurity.com/2017-Credential-Spill-Report-w.html.

[48] Lev Grossman, "Inside Apple's Code War," *Time*, March 28, 2016, 44.

[49] Ibid, pp. 44-49.

[50] "Edward Snowden: Leaks that exposed US spy programme," *BBC News*, January 17, 2014, accessed May 6, 2017, http://www.bbc.com/news/world-us-canada-23123964.

[51] "Computing Education and Future Jobs: National, State & Congressional District Data," *National Center for Women & Information Technology*, accessed April 11, 2017, https://www.ncwit.org/edjobsmap.

[52] Executive Office of the President of the United States, President's Council of Advisors on Science and Technology, *Engage to Excel: Producing One Million Additional College Graduates With Degrees in Science, Technology, Engineering, and Mathematics* (February 2012): i.

[53] Alan Neuhauser, "Foreign Students Outpacing Americans for STEM Graduate Degrees," *U.S. News & World Report*, May 17, 2016.

[54] US Department of Commerce, Economics and Statistics Administration, *Women in STEM: A Gender Gap to Innovation* (Washington, DC: August 2011): 2-4.

[55] "Women, Minorities, and Persons with Disabilities in Science and Engineering," *National Science Foundation*, accessed April 10, 2017, https://www.nsf.gov/statistics/2017/nsf17310/.

[56] Ibid.

[57] Barack Obama, National Security Strategy, (Washington D.C.: White House, February 2015).

[58] Ibid.

[59] "Computer security is broken from top to bottom," *The Economist*, April 8, 2017, http://www.economist.com/news/science-and-technology/21720268-consequences-pile-up-things-are-starting-improve-computer-security.

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Dan Steinbock, "The erosion of America's defense innovation," *American Foreign Policy Interest*, Jan 20, 2015, vol. 36, p. 366-374.

[64] Ibid.

[65] Ibid.

[66] "IT industry outlook 2016," *CompTIA*, https://www.comptia.org/resources/it-industry-outlook-2016-final, January 2016.

[67] "Virtual reality in healthcare," *Virtual Reality Society*, https://www.vrs.org.uk/virtual-reality-healthcare, accessed on May 11, 2017.

[68] Ibid.

[69] Carl B. Frey and Michael A. Osborne, "The future of employment: how susceptible are jobs to computerisation?" *Oxford Martin School, University of Oxford*, September 17, 2013.

[70] Ibid.

[71] Ibid.

[72] Jane Wakefield, "Foxconn replaces '60,000 factory workers with robots'," BBC, http://www.bbc.com/news/technology-36376966 (accessed April 11, 2017).

[73] "The third great wave," *The Economist*, http://www.economist.com/news/special-report/21621156-first-two-industrial-revolutions-inflicted-plenty-pain-ultimately-benefited, October 3, 2014.

[74] Ibid.

[75] Farhad Manjoo, "Tech's 'frightful 5' will dominate digital life for foreseeable future," *The New York Times*, January 20, 2016, https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html?_r=0.

[76] Ibid.

[77] Clayton M. Christensen, *The Innovator's Dilemma—When New Technologies Cause Great Firms to Fail*, (Boston: Harvard Business Review Press, 2011).

[78] Ibid.

[79] Ibid.

[80] White House, "The Comprehensive National Cybersecurity Initiative," The White House, accessed May 8, 2017, https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

[81] Arian Croft, "EU Threatens to Suspend Data-sharing with US Over Spying Reports," Rueters, accessed May 11, 2017, http://www.reuters.com/article/usa-security-eu-idUSL5N0FB1YY20130705.

[82] Alec Ross, *The Industries of the Future*, (New York, NY: Simon & Schuster Paperbacks, 2016), 153.

[83] Mark Gerencser, "Big Data: Dream or Potential Nightmare," University of Maryland University College, last modified 2017, accessed April 16, 2017, http://www.umuc.edu/documents/upload/big-data-dream-or-nightmare.pdf.

[84] Ibid.

[85] David Cohen, "How Facebook Manages a 300-Petabyte Data Warehouse, 600 Terabytes Per Day," April 11, 2014, accessed April 16, 2017, http://www.adweek.com/digital/orcfile/?red=af; "Newsroom," Facebook, last modified 2017, accessed April 15, 2017, https://newsroom.fb.com/company-info/.

[86] Information and Communications Technology Industry Study Domestic Field Studies, April 3-6, 2017.

[87] Department of Defense, Cyberspace Operations, Joint Publication 3-12 (Washington, DC: Joint Chiefs of Staff, February 5, 2013), II-5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed April 18, 2017); the Department of Defense defines cyberspace attacks as those:

> [c]yberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains. These specific actions are:
>
> (a) Deny. To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.
>
> 1. Degrade. To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified.
> 2. Disrupt. To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent.
> 3. Destroy. To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.
>
> (b) Manipulate. To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.

[88] Information and Communications Technology Industry Study Domestic Field Studies, April 3-6, 2017.

[89] "2016 Data Breach Investigation Report," Verizon, 8, accessed April 19, 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[90] Ibid, p. 9.

[91] "Key Findings," Shape, last modified 2017, accessed April 20, 2017, http://info.shapesecurity.com/2017-Credential-Spill-Report-w.html.

[92] "Multifactor authentication (MFA)," SearchSecurity, last modified 2017, accessed April 19, 2017, http://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.

[93] "Multi-factor authentication: A technology whose time has finally come," Deloitte, 2, accessed April 20, 2017, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-deloitte-multi-factor-authentication.pdf; Google Authenticator, iTunes Store, last modified 2017, accessed April 19, 2017, https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8.

[94] James Clapper, Marcel Lettre, and Mike Rogers, "Joint Statement for the Record, Janurary 5, 2017," Senate Armed Services Committee, 3, accessed April 22, 2017, https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf.

[95] US President, "Presidential Policy Directive-21: Critical Infrastructure Security and Resilience," White House Archives (February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed April 11, 2017); the sixteen critical infrastructure sectors and relevant sector-specific agency (SSA) defined in Presidential Policy Directive-23 (Critical Infrastructure Security and Resilience) include:

1. Chemical (SSA: Department of Homeland Security)
2. Commercial Facilities (SSA: Department of Homeland Security)
3. Communications (SSA: Department of Homeland Security)
4. Critical Manufacturing (SSA: Department of Homeland Security)
5. Dams (SSA: Department of Homeland Security)
6. Defense Industrial Base (SSA: Department of Defense)
7. Emergency Services (SSA: Department of Homeland Security)
8. Energy (SSA: Department of Energy)
9. Financial Services (SSA: Department of the Treasury)
10. Food and Agriculture (co-SSAs: U.S. Department of Agriculture and Department of Health and Human Services)
11. Government Facilities (co-SSAs: Department of Homeland Security (DHS) and General Services Administration)
12. Healthcare and Public Health (SSA: Department of Health and Human Services)
13. Information Technology (SSA: Department of Homeland Security)
14. Nuclear Reactors, Materials, and Waste (SSA: Department of Homeland Security)
15. Transportation Systems (co-SSAs: DHS and Department of Transportation)
16. Water and Wastewater Systems (SSA: Environmental Protection Agency).

[96] Information Sharing Environment, "Critical Infrastructure and Key Resources," Office of the Program Manager for the Information Sharing Environment, accessed April 12, 2017, https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources.

[97] US President, "Presidential Policy Directive-21: Critical Infrastructure Security and Resilience," White House Archives, February 12, 2013, accessed April 11, 2017, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[98] Critical Infrastructures Protection Act of 2001.

[99] William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September 2010): 97-108, EBSCOhost, accessed December 14, 2016; also referenced in Brady Stout, "Securing Cyberspace While Balancing Government Control and Public Privacy," Dwight D. Eisenhower School for National Security and Resource Strategy, 5.

[100] Thomas Rid, "Cyberwar and Peace," *Foreign Affairs* 92, no. 6 (November 2013): 77-87, EBSCOhost (accessed December 14, 2016); also referenced in Brady Stout, "Securing Cyberspace While Balancing Government Control and Public Privacy," Dwight D. Eisenhower School for National Security and Resource Strategy, 5.

[101] Electricity-Information Sharing and Analysis Center, "Analysis of the Cyber Attack on the Ukrainian Power Grid," North American Electric Reliability Council, accessed April 18, 2017, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf; Jamie

Condliffe, “Ukraine’s Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks,” Massachusetts Institute of Technology(MIT) Technology Review, accessed April 20, 2017, https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

[102] Ibid.

[103] Clapper, Lettre, and Rogers.

[104] Critical Infrastructures Protection Act of 2001.

[105] Cleve R. Wootson Jr., “Most Cybersecurity Experts Are Worried About Russian Hackers. One Says: Look, a Squirrel!,” Washington Post, accessed April 19, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/01/18/most-cybersecurity-experts-are-worried-about-russian-hackers-one-says-look-a-squirrel/?utm_term=.6023d3bd736d; and CyberSquirrel, “Cyber Squirrel 1,” CyberSquirrel, http://cybersquirrel1.com.

[106] JR Minkel, “Years Later,” *Scientific American*, https://www.scientificamerican.com/article/2003-blackout-five-years-later/ (accessed April 16, 2017).

[107] "IBM - What is Big Data?" IBM, accessed April 6, 2017. https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html.

[108] *Commandant Lecture Series, Eisenhower School for National Security and Resource Strategy*, April, 2017.

[109] "Big Data: A Road Map for Business Intelligence," MarketLine Advantage, last modified 2015/03/05, http://advantage.marketline.com.nduezproxy.idm.oclc.org/Product?ptype=Case+Studies&pid=ML00019-004.

[110] "IBM - What is Big Data?"

[111] Babak Akhgar, *Application of Big Data for National Security: A Practitioner’s Guide to Emerging Technologies* (Oxford, UK: Butterworth-Heinemann, 2015).

[112] *Big Data and Data Analytics - the Potential for Innovation and Growth*

[113] "IBISWorld Industry Report 51121c - Business Analytics & Enterprise Software Publishing," IBISWorld, last modified February, http://clients1.ibisworld.com.nduezproxy.idm.oclc.org/reports/us/industry/default.aspx?entid=1989.

[114] Ibid.

[115] Ibid.

[116] Ibid.

[117] Nicolaus Henke, Ari Libarikian and Bill Wiseman, "Straight Talk about Big Data," *McKinsey Quarterly*, no. 4 (October 2016), 42-51.

[118] Roger Clarke. "Big Data, Big Risks," *Information Systems Journal* 26, no. 1 (January 2016), 77-90. doi:10.1111/isj.12088.

[119] Bart Baesens et al, "Transformational Issues of Big Data and Analytics in Networked Business," *MIS Quarterly* 40, no. 4 (12, 2016), 807-818.

[120] Libarikian Henke and Wisema, *Straight Talk about Big Data*, 42-51

[121] *The Enterprise Lacks a Big Data Strategy for IoT Transformation,* Harvard Business Review, January 29, 2017.

[122] Brad Lackey, *Quantum Computing Presentation to Eisenhower School ICT Seminar,* March 7, 2017; *IBM Watson to Eisenhower School ICT Seminar*, February 24, 2017.

[123] Big Data and Data Analytics - the Potential for Innovation and Growth

[124] Ibid.

[125] K.I.M. Gang-Hoon, Silvana Trimi and Ji-Hyong Chung. "Big-Data Applications in the Government Sector," *Communications of the ACM* 57, no. 3 (March 2014), 78-85. doi:10.1145/2500873.

[126] Information and Communications Technology Industry Study International Field Studies, April 25-28, 2017.

[127] Big Data and Data Analytics - the Potential for Innovation and Growth.

[128] Ibid.

[129] Akhgar, *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies.*

[130] Gang-Hoon, Trimi and Ji-Hyong Chung, *Big-Data Applications in the Government Sector*, 78-85.

[131] Ibid.

[132] Douglas O. Linder, "The Right of Privacy," The Right of Privacy: Is it Protected by the Constitution? accessed May 02, 2017, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

[133] "Olmstead v. United States (1927)," Bill of Rights Institute, accessed April 14, 2017, https://billofrightsinstitute.org/educate/educator-resources/lessons-plans/landmark-supreme-court-cases-elessons/olmstead-v-united-states-1927/.

[134] The Act is formally known as The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015.

[135] Greene, Robyn. "Incidental Collection is Extremely Troubling, Regardless of Legality." March 24, 2017. (Accessed May 10, 2017). https://www.justsecurity.org/39226/incidental-collection-extremely-troubling-legality/; incidental collection is a circumstance in which the government collects the communications of a U.S. person. In these cases, the U.S. person collection is typically unintentional with data being captured in collection "about" a target. For example, the FISA act requires the government to target specific selection terms in programming collection tasks. If, however, that specific selector is not specific enough, when entered by analysts, then the collection enterprise may also gather unintended communications which could include that of U.S. persons

[136] Martin A. Weiss, Kristin Archick, "U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield: R44257," *Congressional Research Service: Report* (May 19, 2016), p. 2, accessed April 5, 2017, https://fas.org/sgp/crs/misc/R44257.pdf

[137] Ibid, p. 2.

[138] Nick Beerman, "A Broadened Crackdown on EU/U.S. Safe Harbor Violations," Jackson Lewis. September 9, 2014, http://www.workplaceprivacyreport.com/2014/09/articles/workplace-privacy/a-broadened-crackdown-on-euu-s-safe-harbor-violations/

[139] Ibid.

[140] Glyn Moody, "Privacy Shield proposed to replace -EU Safe Harbor, faces skepticism," *Ars Technica UK*, 29 February 2016, http://arstechnica.com/tech-policy/2016/02/privacy-shield-doomed-from-get-go-nsa-bulk-surveillance-waved-through/

[141] Ibid.

[142] Farhad Manjoo, "Right to Be Forgotten Online Could Spread," *New York Times*, August 5, 2015, https://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=0

[143] Peter Sayer, "EU gives companies two years to comply with sweeping new privacy laws", cio.com, April 14, 2016, http://www.cio.com/article/3056699/eu-gives-companies-two-years-to-comply-with-sweeping-new-privacy-laws.html

[144] *Freedom on the Net 2016*, Washington, DC: Freedom House, 2016: p. 194.

[145] "500 Retweets Will Now Get You Three Years in Prison in China – Global Voices," Global Voices. September 13, 2013, accessed May 02, 2017, https://globalvoices.org/2013/09/12/500-retweets-will-now-get-you-three-years-in-prison-in-china/.

[146] "Creating a digital totalitarian state; China's social-credit system," *The Economist*, 17 December 2016, p. 20. *Biography in Context*, nduezproxy.idm.oclc.org/login?url=http://link.galegroup.com/apps/doc/A473976724/BIC1?u=wash60683&xid=853c03b8. Accessed 2 May 2017.

[147] Freedom House, p. 2.

[148] General Accountability Office, *DoD Major Automated Information Systems: Improvements Can Be Made in Applying Leading Practices for Managing Risk and Testing, March 2017*, (GAO-17-322, Washington, DC), 1.

[149] Ibid.

[150] Alex Haber, "Attacking the root of the problem in DoD acquisitions," *The Hill.com*, January 12, 2015, accessed April 10, 2017, http://thehill.com/blogs/congress-blog/homeland-security/229046-attacking-the-root-of-the-problem-in-dod-acquisitions

[151] Fred Kaplan, "Procuring Innovation," *MIT Technology Review*, Vol 120, no. 1, (January 2017): 69, accessed April 7, 2016, https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/

[152] U.S. Department of the Defense, *Defense Innovation Unit Experimental (DIUx)l How-to-Guide*, DIUx, November 30, 2016, 1.

[153] Other Transaction Authority, U.S. Code 10 (2015), Section 2371b(f).

[154] Information and Communications Technology Industry Study Domestic Field Studies, April 3-6, 2017.

[155] Fred Kaplan, "Procuring Innovation." *MIT Technology Review*, Vol 120, no. 1, (January 2017): 69, accessed April 7, 2016, https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/

[156] Ibid, p. 71.

[157] Jerry McGuire movieclip, http://www.bing.com/videos/search?q=youtube+show+me+the+money&view=detail&mid=EB19CD9CD9DC3004F33FEB19CD9CD9DC3004F33F&FORM=VIRE

[158] "Jerry Maquire," Wikipedia – The Free Encyclopedia, https://en.wikipedia.org/wiki/Jerry_Maguire

[159] Human Capital, Oxford Dictionary, http://www.oxfordlearnersdictionaries.com/definition/english/human-capital

[160] Gil Press, "A Very Short History of Information Technology (IT)," Forbes. June 18, 2013, accessed April 11, 2017, https://www.forbes.com/sites/gilpress/2013/04/08/a-very-short-history-of-information-technology-it/#6b53a92f2440.

[161] Information and Communications Technology Industry Study Domestic Field Studies, April 3-6, 2017.

[162] Cisco and FireEye specifically noted examples, while Google encourages its employees to share their skills with their colleagues. They promote a 20% program where for that time at work, with approval, they can contribute to other activities such as planning off-sites, teaching yoga, and gardening.

[163] Vivian Hunt, Dennis Layton, and Sara Prince, "Why Diversity Matters," January 2015, http://www.mckinsey.com/business-functions/organization/our-insights/why-diversity-matters

[164] Meghan M. Biro, "Women In Technology: Why It's Good For Everyone," Forbes, April 27, 2015, accessed April 13, 2017, https://www.forbes.com/sites/meghanbiro/2015/04/27/women-in-technology-why-its-good-for-everyone/#37cffb6a7cbb.

[165] Katherine W. Phillips, "How Diversity Makes Us Smarter," Scientific American, September 10, 2014, accessed April 3, 2017, https://www.scientificamerican.com/article/how-diversity-makes-us-smarter/.

[166] "Girls Who Code: Annual Report 2016," Who Code - Annual Report 2016, accessed April 11, 2017, https://girlswhocode.com/2016report/#programs.

[167] Ibid.

[168] Ibid.

[169] Farhad Manjoo, "Tech's 'Frightful 5' will dominate digital life for foreseeable future," *The New York Times*, https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html?_r=0, January 20, 2016.