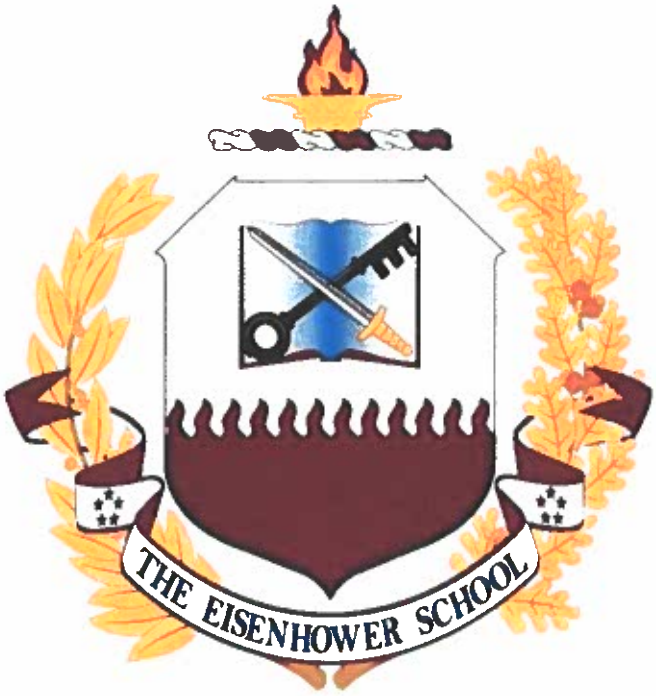
Spring 2018 Industry Study

Final Report

Information and Communications Technology



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

19-S-0829

INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) 2018

ABSTRACT: The information and communications technology (ICT) industry is a driver of economic growth, an essential enabler of other industrial sectors, and a source of rapid and disruptive innovation. ICT is at the heart of the 4th Industrial Revolution, defined as convergence of the digital, physical, and biological worlds. Individual research and visits to ICT firms and institutions in the Washington, DC, area, California, China, and South Korea revealed that, while the U.S. remains the global leader in the ICT field, it faces intense competition from foreign competitors fully committed to winning the race for technological supremacy. Policymakers should focus on strengthening public-private collaboration and modernizing outdated regulatory structures to address national security needs while fostering the entrepreneurial environment that has allowed the U.S. ICT sector to thrive and lead globally.

Lt. Col. Charles Bris-Bois	United States Air Force
Lt. Col. Patrick Dagon	United States Army
Mr. Kevin Donovan	Federal Bureau of Investigation
Mr. Paul Fritch	Department of State
Mr. Kenneth Graf	United States Secret Service
Mr. Mark Harrington	Department of Homeland Security
Lt. Col. Gregory Pace	United States Marine Corps
Col. Amado Sanchez	United States Army
Lt. Col. Paul Sebold	United States Air Force
Ms. Maura Styczynski	Department of the Navy
Col. Jaak Tarien	Estonian Air Force
Lt. Col. Emmanuel Thome	French Defense Procurement Agency (DGA)
Lt. Col. Ryan Vetter	United States Air Force
Ms. Marika Zadva	Department of State

Col Paul Gillespie, PhD	U.S. Air Force, Faculty Lead
Mr. Richard Altieri, J.D.	Faculty
Mr. Stephen Bloor, J.D.	Faculty
Mr. Thomas Olohan, J.D.	Faculty

Industry Study Outreach and Field Studies

On-Campus Presenters:

Federal Communications Commission (FCC), Washington, DC
National Telecommunications & Information Agency (NTIA), Washington, DC
U.S. Patent & Trademark Office, Washington, DC
Microsoft, Washington, DC
Joint Center for Quantum Information and Computer Science, College Park, MD
Diffeo Inc., Cambridge, MA
NAV Venture Capital, Reston, VA
FirstNet, Washington, DC
J Capital Research, New York, NY

Field Studies—Domestic:

Sirius XM, Washington, DC
Starship, Washington, DC
Information Technology Industry Council (ITIC), Washington, DC
Cellular Telecommunications and Internet Association (CTIA), Washington, DC
Dell EMC, McLean, VA
Verizon, Ashburn, VA
Central Intelligence Agency (CIA), Langley, VA
National Security Agency (NSA), Ft. Meade, MD
U.S. Cyber Command (USCYBERCOM), Ft. Meade, MD
Laboratory for Telecommunication Sciences (NSA), College Park, MD
Army Research Labs, College Park, MD
Department of Homeland Security, Arlington, VA
Defense Information Systems Agency, Ft. Meade, MD
Cisco, San Jose, CA
Facebook, Menlo Park, CA
Google, Mountain View, CA
Hewlett Packard, Palo Alto, CA
NASA Ames Research Center, Moffett Field, CA
Oracle, Redwood City, CA
Stanford University, Stanford (Palo Alto), CA
Shape Security, Mountain View, CA

Field Studies – International:

U.S. Consulate General, Hong Kong, People's Republic of China (PRC)
Hong Kong University of Science and Technology, Big Data Institute, Hong Kong, PRC
Applied Science and Technology Research Institute (ASTRI), Hong Kong, PRC
Huawei, Shenzhen, PRC
UBTech, Shenzhen, PRC
IngDan, Shenzhen, PRC

TCL, Shenzhen, PRC
TimeKettle, Shenzhen, PRC
DJI, Shenzhen, PRC
U.S. Embassy Seoul, Seoul, Republic of Korea (ROK)
Korea Internet and Security Agency, Seoul, ROK
Samsung SDS, Seoul, ROK
LG – Science/Digital Park, Seoul, ROK

Introduction

The information and communications technology (ICT) industry is characterized by rapid and disruptive innovation, which constantly redefines industry segments, the market, and the boundaries of the industry itself. More than any other industry studied by the Eisenhower School (with the exception of healthcare), ICT also has a direct and tangible impact on the lives of American citizens. A mere 11 years after the introduction of Apple's first iPhone, 77% of Americans now carry smartphones.[1] Web searches, satellite navigation, social media, and other transformative technologies have become essential elements of daily life within the space of a single generation, with similar breakthroughs – driverless cars, artificial intelligence/machine learning, homes networked through the "Internet of Things" (IoT) – either in the early adopter phase or just over the horizon. ICT firms themselves include five of the six most valuable American companies, and encompass 7.5% of the economy (some 5.5 million jobs). Yet the importance of a healthy ICT sector goes well beyond these numbers, given the reliance of virtually all other industries (including government and the military) on ICT infrastructure to conduct day-to-day business.

The ubiquity of ICT, and its rapid technological development, pose several policy challenges, including: how best to foster a business climate that keeps the U.S. on the cutting edge of new technologies; how to develop (and attract) the human capital necessary to sustain a vibrant and innovative ICT sector; how best to adapt the acquisition process to leverage potentially transformative technologies for military and security purposes; how best to protect critical national infrastructure that is increasingly reliant on ICT; how to anticipate, deter, prevent, and respond to potential threats in cyberspace; and how to balance security and privacy in an era when astonishing amounts of sensitive personal data are aggregated and potentially available online.

Given the magnitude of these challenges, and the constantly evolving state of the ICT industry, this study does not purport to be comprehensive. Nonetheless, the 2018 ICT Industry Seminar, through independent research, interactions with government and industry representatives in the Washington, DC, area, and field visits to leading technology firms in California, China, and South Korea, attempted to identify and analyze some key challenges the industry poses to policymakers and to put forward concrete recommendations to address them.

The Industry Defined

Overview: The ICT industry is broadly defined as software (18%), devices and infrastructure (17%), information technology (IT) services (31%), other emerging technology (12%), and telecommunications services (23%).[2] For the purposes of industry analytics, the Seminar examined four major firms: Cisco, Oracle, Verizon and Alphabet/Google, and while they are representative of the five major categories of the ICT industry, they comprise only a small portion of the 388,000 U.S. companies that employ approximately 5.5 million people and represent 7.5% of the U.S. economy with $1.5T in revenue in 2018.[3] According to 2017 data, five of the six most valuable American companies are in the ICT sector.[4] Additionally, the ICT industry accounted for more than 25% of U.S. economic growth from 1995 to 2009, and the Information Technology and Innovation Foundation estimates that as of 2010, ICT in general had made the U.S. economy approximately $2 trillion larger in terms of annual GDP than it would be otherwise.[5] Furthermore, the U.S. leads the world in aggregating ICT research and development (R&D) investment, with more than half of worldwide spending ($122 billion

compared to estimated global spending of $218 billion in 2017).[6] Companies within the industry have revenue streams that span multiple North American Industry Classification System (NAICS) codes, to include Telecommunication Networking Equipment Manufacturing in the U.S. (33421) Database, Storage and Backup (51121b), Wireless Telecommunications Carriers (51721) and Satellite Telecommunications (51741), to name just a few. The defining characteristic of all the companies studied and visited by the Seminar is their recognition that they must continuously innovate to stay in front of the competition, and therefore tend to spend a considerably larger portion of their revenue on R&D. Virtually all of the companies analyzed are vying to become industry leaders in the 4th Industrial Revolution, defined as the convergence of the digital, physical, and biological worlds. ICT companies are particularly interested in developing and exploiting disruptive technologies such as artificial intelligence/machine learning, big data, 5G wireless, and cloud computing.

The Current Condition of the Industry

In the U.S., the telecommunications sector of the industry is dominated by the 'Big Four' (Verizon/AT&T/T-Mobile/Sprint, with T-Mobile and Sprint currently engaged in merger negotiations). The sector's revenue in 2017 decreased to $79B (down 6% from 2016), which highlights the extreme competitiveness within the sector. Firms in the industry face large infrastructure investment requirements, especially as standards within 5G are solidified. As a result, the barriers to entry in this sector of the industry are extremely high. Meanwhile, relatively new players – notably Amazon, Alphabet/Google, and Facebook – have leveraged new technology to create entirely new markets (online retail, web search, and social media, respectively), in the process establishing themselves among the nation's (and the world's) most valuable companies and securing a level of market dominance that has prompted calls for increased government regulation (with some even advocating anti-trust action).[7]

Strong global competition, particularly from Chinese firms such as Huawei Technologies and ZTE Corporation, will continue to drive down communications equipment prices. Operators within the industry continue to morph and expand services, shifting the competitive landscape and requiring firms to continue to prioritize R&D efforts. Arriving late to market can make the difference between being in the top five and dropping out of the top ten.

A Porter's Five Forces analysis of the ICT industry demonstrates that most of its segments are converging, as IT services continue to merge, and firms move to provide services remotely through "cloud" technology (see below). As a result, leaders in the various segments, including Verizon and AT&T (telecommunications), Cisco (network equipment manufacturing), Oracle (Enterprise Resource Planning), Alphabet/Google (search engines), and Amazon Web Services and Microsoft Azure (cloud computing), have become competitors in the emerging ICT landscape. For example, firms such as Verizon and Google, which previously were not true competitors, now find themselves as rivals following Google's entry into the wired telecommunication segment in multiple states with their Google Fiber service. Against this backdrop, competitive pressures are high across the ICT industry. Although we see new entrants in the various ICT segments in the form of the crossover described above, the threat to established firms of new entrants from *outside* the ICT industry is generally low due the intensive capital requirements necessary to gain market share. The threat of substitution across the ICT industry is generally high because of the ability to quickly reproduce/improve substitute software, device infrastructure, and IT services. Buyer power is high across the industry because of the numerous product/service options and the ability for customers to switch easily between

developers, providers, and/or manufacturers. Supplier power is generally weak because of the large number of suppliers and the undifferentiated nature of inputs among various suppliers.

The ICT industry is also uniquely vulnerable to international economic and regulatory pressures, due both to the transnational nature of cyberspace and the focus on future growth. As the use of key technologies reaches saturation in the U.S., Europe, and other mature economies, the majority of potential growth for much of the ICT sector is in the developing world: "In 2013, a median of 45% across 21 emerging and developing countries reported using the internet at least occasionally or owning a smartphone. In 2015, that figure rose to 54%, with much of that increase coming from large emerging economies such as Malaysia, Brazil, and China. By comparison, a median of 87% use the internet across 11 advanced economies surveyed in 2015, including the U.S. and Canada, major Western European nations, developed Pacific nations (Australia, Japan, and South Korea) and Israel. This represents a 33-percentage-point gap compared with emerging and developing nations."[8] This increasing reliance on international sales as a primary source of revenue growth creates potential vulnerabilities to foreign regulation on international property, data privacy, and other issues.

A vibrant ICT industry is essential for national security and prosperity, and the Seminar's work revealed a need for U.S. government policy focus in the following four areas:

- Fostering innovation and economic growth;
- Maximizing the efficient use of new technologies for government, military, and national security purposes, and securing U.S. government and commercial ICT infrastructure;
- Managing the implications of global supply chains; and
- Balancing constitutional rights (in particular personal privacy) and national security.

Fostering Innovation and Economic Growth

The Seminar had the opportunity to study a number of emerging technologies, which can be expected to disrupt the ICT sector, and the U.S. and global economies more broadly, in the coming years. Attaining and preserving a decisive technological edge in these fields is essential to future U.S. economic growth, while the rapid adoption of new technologies by government agencies and the military is critical to national security. The Seminar studied several areas of current or imminent technological breakthrough relevant to American security and prosperity, including:

- *5G:* The development of fifth-generation wireless technology (5G) is expected to provide a key enabler for other transformative technologies, such as self-driving cars, smart sensors, thermostats, networked robots, smart cities, virtual reality, and remote medical procedures.[9, 10] 5G will provide phones and other networked mobile devices with a stable connection roughly10x faster than 4G,[11] enabling real-time communication with little to no "latency" (lag time between signal generation and signal reception). If successfully implemented, this will permit technologies currently relegated to laboratories and small-scale pilot projects to come into more general use. 5G technology also has extensive potential military uses, and could significantly reduce the number of personnel required in battlefield environments by increasing access to real-time intelligence. Several U.S. ICT firms, including Verizon (VZ), AT&T (T), T-Mobile (TMUS) and Sprint (S),[12] are currently engaged in the development and testing of 5G technology, and this effort featured prominently in visits to ICT firms in

China (Huawei, TCL) and Korea (Samsung). The increasing ubiquity of 5G technology, particularly to the extent that foreign firms play a leading role in R&D, raises concerns about cybersecurity and privacy. At its full potential, 5G will mean that information about almost every aspect of our lives could be recorded and stored in the cloud.[13]

- *Spectrum Management:* The development of 5G and other emerging technologies will require enhanced efficiency in the allocation of the electromagnetic spectrum. The "electromagnetic spectrum (ES) is the entire range of wavelengths or frequencies of electromagnetic radiation extending from gamma rays to the longest radio waves and including visible light" used for nearly everything that sends a signal through the air or relies on receiving a signal in order to accomplish its task.[14] Efficiency is critical as it is estimated that, "by 2019, the U.S. will see a 78-fold increase in wireless data use over the 2010 level. Taking into account additional infrastructure and increased spectral efficiencies, CTIA has calculated the amount of additional licensed spectrum – over 350 MHz – necessary by the end of the decade to meet this explosion in mobile data."[15] Private industry has a vested interest in improving the efficiency of spectrum use, and the talent exists in the private sector to develop new technologies that provide greater efficiency in managing the spectrum. The government should harness this talent and continue to pursue the development of technology for sharing when it is not needed 100% of the time and does not degrade the mission.

- *Cloud Computing:* Cloud computing is an emerging disruptive technology aimed at displacing legacy IT architecture in favor of rapid scalability, flexibility, on-demand accessibility, and consumption based on a pay-as-you-go business model. Cloud computing permits government and commercial clients to contract application processing and data storage from cloud service providers instead of owning and maintaining these capabilities internally. While some aspects of cloud computing could enhance overall security by reducing the attack surfaces of the network, many experts in the field contend that information stored in a cloud environment is at higher risk of being hacked because large quantities of information are aggregated in a single location on the Internet. While U.S. firms, including Amazon, Microsoft, Google, and Oracle, currently maintain an edge in cloud infrastructure, foreign competitors (including Huawei and Samsung) are seeking a foothold in this emerging market. The U.S. government (including the military) will need to preserve the competitive edge of the National Security Innovation Base (NSIB), and take advantage of the opportunities offered by cloud technology for efficiency and rapid technological development while addressing specific security concerns.

- *"Big Data":* The 2017 National Security Strategy acknowledged that "the ability to harness the power of data is fundamental to the continuing growth of America's economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world."[16] A term coined in the 2000s, big data has come to refer to "vast, constantly increasing amounts of digital information used to [among other things] optimize business processes, create customer value, and mitigate risks."[17] Big data done right has the potential to help organizations identify where their workers and business processes are performing sub-optimally, illuminate what options have the best probability of helping them succeed, reduce risk, and ultimately cut costs.[18] Unfortunately, opportunists have discovered ways to

capture and sell increasing amounts of our data, and this 21st century "gold rush" has brought ethical and moral dilemmas regarding privacy to light with which we are only now starting to grapple. Striking the delicate balance between data optimization/open e-commerce, data security, and respecting people's right-to-privacy online will determine how successful U.S. industry will be compared with foreign competitors in the coming age.

- *Artificial Intelligence/Machine Learning:* China is investing billions of dollars into R&D on artificial intelligence/machine learning (AI/ML), with little to no concern for ethical considerations, and the U.S. is in danger of being left behind in an innovation sector essential to the future NSIB. Policy makers and elected officials will need to consider how best to advance R&D into this cutting-edge technology while ensuring ethical concerns remain a priority. Although not a specific focus of this year's industry study, the centrality of AI/ML to further technological development, and the danger of being left behind in the face of massive Chinese investment, were common threads that emerged during several CONUS and OCONUS field visits. In the coming years, the ICT Industry Study should include targeted visits to AI/ML firms, aimed at providing recommendations to future policy makers in this vital area.

In addition to the R&D areas outlined above, all of the Seminar's government and firm visits revealed an urgent need to focus on *human capital,* both within the U.S. government and in the economy more broadly. Maintaining a technological edge in the ICT industry will require the maintenance and growth of a skilled workforce. U.S. government policy should seek to incentivize U.S. students, beginning at the K-12 level, to pursue careers in Science, Technology, Engineering, and Math (STEM) fields, while reforming the immigration system to ensure that the U.S. continues to attract elite talent from throughout the world. The U.S. must maintain a steady flow of qualified STEM graduates and continually strive to improve the education system so that all U.S. graduates receive the best education possible at all skill levels. One problem impacting the U.S. education system is the lack of homogeny in terms of quality education across states and economic levels. To supplement traditional education programs, private industry has been partnering with government and educational institutions to offer apprenticeships and alternate degree programs to address the gap between the skills that universities provide and the job requirements of employers. Successful programs like IBM's Pathways in Technology Early College High Schools (P-TECH), which "are innovative public schools spanning grades 9 to 14 that bring together the best elements of high school, college and career,"[19] must be expanded; 100 such schools are far too few for a nation the size of the U.S. An independent and credible body that tracks and assesses trends and prospects for education and careers in science and engineering (S&E) fields is also needed[20] so that policy decisions can be based on independent assessments, rather than biased reports generated by industry and lobbying firms. Repeated studies by Rand Corporation concluded that there is not a shortage of S&E labor, but that better data collection is required in order to provide empirical statistics.[21]

Maximizing the Efficient Use of New Technologies for Government, Military, and National Security Purposes, and Securing U.S. Government and Commercial ICT Infrastructure

In addition to the industry-wide issues outlined above, the Seminar identified several issues specific to the U.S. Government (including the military), its role in protecting critical public and private infrastructure, its procurement processes, and its efforts to deter and prevent

cyber threats. These include:

- *Reforming Department of Defense (DoD) ICT Acquisition:* The U.S. ICT industry creates millions of jobs and serves as a strong driver for innovation, research, and development, yet the defense sector does not fully leverage this flourishing sector. In 2013, the "Big Five" defense contractors – Lockheed Martin, Boeing, Raytheon, General Dynamics, and Northrop Grumman – accounted for approximately 30% of DoD contract obligations, exceeding $500 million in annual obligations.[22] High-tech firms outside the traditional defense sector are reluctant to engage the DoD due to high regulatory burdens, limited potential, intellectual property (IP) issues, lack of transparency, and long product development times. In order to harness the potential of the U.S. ICT sector, DoD must urgently lower barriers to entry to enable small and non-traditional defense companies to bid on defense contracts. Beyond process, a massive cultural divide also prevents the Pentagon from attracting cutting-edge innovations. According to Steve Jobs, "innovation has nothing to do with how many R&D dollars you have. When Apple came up with the Mac, IBM was spending at least 100 times more on R&D. It is not about money. It's about the people you have, how you're led, and how much you get it."[23] This cultural barrier is fundamentally rooted in human capital, and requires a change of mindset in the federal acquisition workforce.

- *Cybersecurity:* Cyber threats and the overall security situation in cyberspace are growing worse. Attackers have gained a strong advantage over defenders, and the vast majority of attacks go unpunished. The general public lacks information, and private sector actors are driven by market incentives to downplay and conceal security breaches. Cyberspace is more abstract than traditional warfighting domains and its nature is changing at a rate that outpaces the government's ability to regulate it properly. Enhancing security will require broad cooperation between private industry, the U.S. government, and international partners to identify trends and protect cyberspace before it is attacked. If we are to overturn the attackers' advantage, we need to adopt a robust, yet agile and adaptive cybersecurity posture across government agencies, and create legal and economic incentives for private industry to do the same. The National Institute of Standards and Technology (NIST) identifies a triad of elements that must be present for cybersecurity: confidentiality, integrity, and availability.[24] Technological developments, like *blockchain*, meet NIST recommendations and hold some promise for enhancing cybersecurity for critical data. Blockchains distribute, rather than aggregate, data through cryptographically-linked chains that provide unrivaled resilience to attacks. Post-quantum cryptography provides an additional layer of protection to data on the blockchain as concerns arise regarding Chinese advancements in quantum computing and the near-term potential for making traditional RSA-based cryptography obsolete. Whether it is increased regulation, financial accountability, or system architecture migration, we must respond to the increasing threat from state and non-state cyber criminals or suffer the consequences to national security.

- *Critical Infrastructure:* The connection to the Internet of previously stand-alone systems that control water supplies and electrical grids make the United States' critical infrastructure extremely vulnerable to cyber-attack. The current voluntary public-private partnership model for addressing cybersecurity within critical infrastructure leaves the country at risk and demonstrates the need for government mandates regarding network monitoring, information sharing, and subsequent inspections/audits to ensure network security within

critical infrastructure. Policy makers need to equip the National Cybersecurity and Communications Integration Center (NCCIC) with the necessary statutory/regulatory authority to ensure implementation of the NIST cybersecurity framework within all critical infrastructure.

Managing the Implications of Global Supply Chains

The Seminar's interactions and events over the course of the semester also highlighted the importance of what some experts say is our greatest future vulnerability – our supply chains. Supply chain risk is defined as "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[25] As firms have focused on their core competencies, outsourcing of manufacturing and critical supply chain responsibilities has mushroomed. Outsourcing has expanded, both domestically and internationally, creating a more tangled web of companies sharing and enabling one another; this creates new challenges in ensuring security in the global supply chain. China's share has increased most dramatically due to inexpensive labor and a responsive manufacturing capability at the expense of domestic production over the past 25 years, leading to:

- Significant risk within the supply chain, including the introduction of components with "back door" vulnerabilities or counterfeit knock-offs (unproven and potentially detrimental);
- A vacuum of institutional experience in domestic manufacturing expertise and capability, with significant national security implications should the United States' overseas sources be cut off or prove untrustworthy; and
- A perceived shortage of qualified STEM experts domestically, leading U.S. companies to look overseas to meet the shortage.

Supply-chain issues are not unique to the U.S. Toward the end of the semester (and coinciding with the Seminar's field visits in the PRC), the U.S. Government restricted the supply of chip sets and processors from U.S.-based Qualcomm to Chinese manufacturer ZTE Corporation over the latter's sales to Iran[26] (a month after the Committee on Foreign Investment in the United States (CFIUS) blocked the acquisition of Qualcomm by Singapore-based Broadcom).[27] ZTE subsequently announced that it would eliminate mobile phone production as a result of this restriction. While this incident indicates that supply-chain vulnerabilities are reciprocal, it also raises the prospect that foreign firms and governments, fearful of eventual U.S. policy intervention, might ultimately develop their own production capabilities for critical technologies, thereby eroding the U.S. technological advantage over time.

Privacy, Security, and Oversight

Finally, the Seminar coincided with a series of high-profile debates about data privacy and security, including the indictment by the Department of Justice (DoJ) Special Counsel of Russian individuals and entities seeking to influence the 2016 Presidential election, the Facebook/Cambridge Analytica scandal, and a wide range of international initiatives to promote data privacy and/or enable government surveillance, including the entry into force of the European Union's General Data Protection Regulation (GDPR) and Chinese forays into "social

credit" monitoring. These developments highlighted the need to update the domestic legal framework with regard to data privacy, and to take a leading role in shaping international norms as practices begin to diverge (with the EU at one end of the spectrum in guaranteeing the privacy of personal data and China at the other in developing ICT as tools of social control). In addition to protecting U.S. national security and IP, and safeguarding the rights of American citizens, U.S. leadership in this area is essential to protecting the economic viability of U.S. ICT firms, which must operate in a wide range of legal and regulatory environments.

China in particular (a focus of the Seminar's work, including April 2018 field visits to Hong Kong and Shenzhen), empowered by indigenous tech giants Alibaba and TenCent, is leveraging its success in ICT innovation in order to enhance social and political control over its populace, and could export its growing expertise in tech-enabled social engineering.[28] The ubiquitous adoption of "super apps" such as Alipay and WeChat has funneled the majority of social, travel, and economic activity from urban Chinese citizens through a duopoly of state-accessible, information collection points.[29] China's advances in facial recognition, smart city monitoring, the IoT, and personal social credit scores are likely to spread to nations looking to gain additional control at the expense of personal liberty. Where this expansion is accompanied by Chinese investment and technology, the nations adopting the systems will also be opening the door to exploitation by the Chinese military and economic intelligence apparatus. Enhanced cooperation with the EU and other like-minded countries to shape international norms is imperative for continued economic growth and sustained U.S. leadership in the ICT industry.

Key Recommendations

As outlined in detail in the issue-specific essays below, the Seminar's work revealed the need for urgent policy action in the following areas:

- Ensure that the U.S. ICT industry retains the ability to develop and attract sufficient human capital to preserve its global leadership role;
- Reform federal acquisition processes to better leverage rapid technological innovation;
- Strengthen the federal role in protecting critical infrastructure and promoting cybersecurity throughout the economy, including by mandating reporting of cyber incidents and cooperation by public and private sector entities with DHS's NCCIC; and
- Update legislation aimed at ensuring data privacy and transparency, and take the lead in establishing accepted international norms in this area.

SELECTED ESSAYS ON MAJOR ISSUES

Innovation, by Lt. Col. Charles Bris-Bois, U.S. Air Force

Why do some nations continuously demonstrate high levels of innovation while others do not? Evidence suggests that the answer lies in a nation's ability to create an environment that incentivizes large financial rewards for: making a product or service better; making a product or service cheaper; or finding a way to do something radically new or different. Innovation in the U.S. has worked best when government provides funding, universities provide talent and training, and the private sector provides the capital needed to move the innovation to market. Innovation occurs at higher rates when R&D is matched with an innovation champion, within an ecosystem that combines five supply conditions (agenda setting, matching, refining, clarifying and routinizing); with five separate demand conditions (relative advantage, compatibility, complexity, trialability, and observability). This process can best be seen through a miniature case study of the innovation of cellphones in the US.

Agenda-setting, the first step in the innovation process, occurs when an organizational problem in need of a solution is first defined.[30] In this case, businessmen needed the ability to remain in touch with their offices and clients while away from their desks. The second step, *matching,* occurs when a technical solution is applied to solving the problem.[31] Creative engineers figured out how to meet the need by mounting large cell phone units in cars. *Refining* happens when the innovation is re-invented to fit the organization's needs.[32] In this case, refining led to cell phones being detached from cars to become hand-held and truly mobile. *Clarifying* occurs when the innovation is put into widespread use. Finally, *Routinization* occurs when the innovation becomes a normal part of regular operations and loses its separate identity.[33] The reasons for the cell phone's rapid adoption and expansion can be explained by the five demand conditions related to cellphone innovation.

The first of the demand conditions for innovation is *relative advantage* – the innovation is perceived as being better than the idea it supersedes, in terms of economic advantage, productivity enhancement, or social prestige.[34] The second demand condition, *compatibility*, is "the degree to which an innovation is perceived as consistent with the existing values, past experiences, and needs of potential adopters."[35] The third demand condition is *complexity*, a measure of how difficult the innovation is to understand and use.[36] The fourth demand condition is *trailability*, the degree to which potential adopters can experiment with the innovation without committing long-term.[37] The final demand condition is *observability*, or the "degree to which the results of an innovation are visible to others."[38]

Understanding the supply and demand conditions of innovation and how R&D and innovation champions can influence the outcome of future conflicts is critical for those who wish to understand the implications of innovation on national security. Understanding the process of innovation has several national security implications, the most important of which is understanding that innovation has and will continue to render existing forms of combat obsolete.[39] States that have the ability to recognize, cope with, and adopt innovation have a significant competitive advantage over those who do not. Simply having access to the latest and greatest technology will not ensure success in future conflicts. As the 2018 National Defense Strategy articulates, "Success no longer goes to the country that develops a new fighting technology first, but rather to the one that better integrates it and adapts its way of fighting."[40]

Spectrum Management, by Lt. Col. Patrick Dagon, U.S. Army

The "electromagnetic spectrum (ES) is the range of wavelengths or frequencies of electromagnetic radiation extending from gamma rays to the longest radio waves and including visible light" used for nearly everything that sends a signal through the air or relies on receiving a signal in order to accomplish its task.[41] "Providing spectrum licenses to support new uses for the airwaves has been a mainstay of spectrum policy since the original Communications Act of 1934."[42] On average, it takes over 13 years to get spectrum into the hands of consumers, due to regulatory and technical requirements, clearing existing users, and testing and deployment.[43, 44] Spectrum efficiency is "the use of the minimum amount of electromagnetic spectrum (EMS) resources necessary to ensure maximum operational effectiveness in fully accomplishing the required mission while taking all practicable steps to minimize impacts to other systems in the electromagnetic environment (EME)."[45] Efficiency is critical as it is estimated that, "by 2019, the U.S. will see a 78-fold increase in wireless data use over the 2010 level. Taking into account additional infrastructure and increased spectral efficiencies, CTIA has calculated the amount of additional licensed spectrum – over 350 MHz – necessary by the end of the decade to meet this explosion in mobile data."[46] In the recent spectrum auction, "the winning bids totaled approximately $20 billion and freed 70 megahertz."[47]

Government's priority is to protect national security interests. DoD defines "spectrum flexibility and adaptability [as] the capability of a spectrum-dependent system (SDS) to exploit various opportunities to access spectrum…. Agile spectrum operations will enable DoD systems to utilize their flexibility and adaptability to achieve mission success in rapidly changing EMEs."[48] "Adversaries are aggressively developing and fielding electronic attack (EA) and cyberspace technologies that significantly reduce the ability of DoD to access the spectrum and conduct military operations."[49] "The Federal government currently occupies – either exclusively or on a primary basis – between 60 and 70 percent of all spectrum in the commercially most valuable range between 225 MHz and 3.7 GHz, which comes to approximately 2,417 megahertz."[50] The USG maintains the ability to takeover certain bands of the electromagnetic spectrum in the case of a national, regional, or local emergency. One trade association's opinion is that DoD understands the productive and economic development advantage that the spectrum provides to the private sector. He indicated that industry has benefited from recent auctions and that the agency has benefited from proceeds from the sale.[51] Two other guest speakers emphasized the importance of DoD in describing and codifying the allocation process.[52]

Private industry has a vested interest in improving the efficiency of spectrum use, and the talent exists in the private sector to develop new technologies that achieve this end. The government should harness this talent and pursue the development of technology for sharing when it is not needed 100% of the time and does not degrade the mission. The Defense Advanced Research Projects Agency (DARPA) is supporting "early research into cognitive radio and dynamic spectrum access through programs such as neXt Generation (XG), and it continues to address key problem areas in spectrum sharing for military systems."[53]

Policy Recommendations:

- Continue to develop policies to assume spectrum control and develop public-private partnerships for infrastructure development (e.g., First Net); offer creative initiatives, such as spectrum or time on the spectrum, as compensation for improved spectrum management; and
- Continue to divest spectrum as the mission and risk analysis allow. Maximize sharing and leasing alternatives, while reducing administrative burden and risk.

The Promise of the Cloud, by Lt. Col. Gregory Pace, USMC

Cloud computing is an emerging disruptive technology that aims to transform how the U.S. government (USG) stores information and accesses software applications, and how it will invest in future IT requirements. Cloud computing aims to displace legacy IT architecture in favor of rapid scalability, flexibility, on-demand accessibility, and consumption based on a pay-as-you-go business model. Cloud computing will allow the USG to contract application processing and data storage from service providers, instead of the current methods of owning and maintaining these capabilities internally. Resource limitations have prompted an enormous push toward shared services and collaboration, especially on back-office functions. Cloud computing provides a vehicle for the USG to become more agile, efficient, flexible and effective with its IT investments. In spite of the many benefits of cloud computing, agencies must address security concerns (data security and privacy concerns), migration considerations, and concerns about legal and regulatory compliance.

Cloud computing security concerns fall into two broad categories: those faced by service providers, and those met by clients. While some aspects of cloud computing could enhance overall security by reducing the attack surfaces of the network, many experts contend that information stored in a cloud environment is at higher risk of being hacked because it is on the Internet. Privacy and confidentiality concerns arise because the service provider has access to data and could accidentally or deliberately disclose it or use it for unauthorized purposes.[54] Coincidentally, the concentration of government information with a cloud service provider presents an attractive target for hackers and increases the impact of a potential data breach. To mitigate security concerns, USG agencies are required to follow the DoD's Risk Management Framework (DoD RMF), the Federal Risk and Authorization Management Program (FedRAMP) and, the DoD Provisional Authorizations.

Secondary to security concerns are cloud migration considerations, which include knowing your current architecture and developing a technology program project, developing a plan to migrate products and/or services to the cloud to include capacity management, performance metrics, historical contractual costs, and understanding the particulars of Service Level Agreements (SLAs).[55] The decision to transition applications or services to the cloud has overarching cost implications (characteristics, delivery model, storage requirements, etc.), but there are also additional cost implications to moving data into the cloud environment, and disruption implications for conceivable internet outages during or after migration.

The future legal and regulatory ramifications of cloud computing services remain mostly unknown, and there are no universal legal requirements regarding protection of information stored on servers located in a municipality, state, or country. Typically, the location of the files confers jurisdiction in the application of legal remedies, e.g., privacy laws, contract laws, and intellectual property laws. However, the site of the company, the location of the user, and the location of the contract also play pivotal roles in determining potential legal remedies. Vigilance must be maintained in legal and regulatory developments in the cloud computing space. The USG will face many challenges in its effort to capture the promise of the cloud. However, with careful and comprehensive planning, these concerns can be mitigated.

Big Data, by Kevin Donovan, FBI

Like previous technological advances, big data has changed the way we work, play, and relate to one another in ways that previous generations never could have predicted. The duration and impact of this high-tech upheaval will depend greatly on the ability of public and private sector leaders to adapt to the fast-changing environment it has created and their willingness to trust vast amounts of unfamiliar data and automated analysis as the basis for their decisions, as opposed to their own experience and instincts. Organizations that fail to adapt and properly and ethically implement data analytics and visualization as a major part of their decision-making model will find themselves at a significant competitive disadvantage.

A term coined in the 2000s, big data refers to "vast, constantly increasing amounts of digital information used to [among other things] optimize business processes, create customer value, and mitigate risks."[56] Sometimes referred to as the 4th Industrial Revolution, digital, physical, and biological systems (to include big data)[57] "blur[] the lines between the physical, digital and biological spheres.[58, 59] Klaus Schwab argues that the current revolution's velocity, scope, and impact distinguish it from its predecessors, particularly because of the disruption it has wrought in every industry in every corner of the globe.[60] Big data done right has the potential to help organizations identify where their workers and business processes are performing sub-optimally, illuminate what options have the best probability of helping them succeed, reduce risk, and ultimately cut costs.[61] Just as previous Industrial Revolutions changed the world in ways that can never be undone, the Digital Revolution of Big Data will continue to challenge long held assumptions, shatter paradigms, and shift balances of power.

The U.S. government, including the DoD, is among the largest collectors of data in the world, so it stands to reason that it should be among the largest contributors to R&D in the field of big data. Much like historical investments in roads and bridges, which fueled this nation's growth and prosperity, the government must spend generously on the virtual infrastructure of the information super-highway to spur growth in the digital age. Growth and jobs go hand-in-hand. Today's jobs, like data scientist, require advanced schooling and diligent application of rigorous standards to ensure that organizations collect the right data, the correct way, with more impactful, error-free results. These tech professionals are increasing user productivity and enhancing their online experience, to the point that billions of personal and business digital transactions now occur seamlessly every day. Unfortunately, with the good comes the bad. Opportunistic entrepreneurs have discovered ways to capture and sell increasing amounts of our data, and this 21st century "gold rush" has brought to light ethical and moral dilemmas regarding privacy with which we are only now starting to grapple. Striking the balance between data optimization/open e-commerce, data security, and respecting citizens' right to privacy online will determine how successful the U.S. can be compared to other nations in the coming age.

Government's Role in Big Data:

The Facebook (FB)/Cambridge Analytica episode has initiated a very public discourse on the responsibility of companies like FB to protect the data with which they are entrusted. Some have suggested that trusting FB to self-regulate is like putting the fox in charge of chicken coop security and that the time has come for government oversight and/or regulation. On April 10, 2018, FB CEO Mark Zuckerberg testified, "It's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy."[62] Signaling that legislation is necessary, Senator Richard Blumenthal (D-Conn.) retorted, "My reservation about your

testimony today is that I don't see how you [FB] can change your business model [which is to monetize user information to maximize profit] unless there are… specific rules and requirements enforced by an outside agency."[63] Blumenthal and Senator Ed Markey (D-Mass.) have proposed a "privacy bill of rights" called the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act, which would empower the Federal Trade Commission (FTC) to create data privacy protections for consumers like mandating that they be given the choice to opt into sharing their personal information instead of having to opt out, as well as requiring companies to inform customers how their data will be used.[64]

Some Representatives are considering a GDPR for the U.S., similar to EU legislation, including better defining "personal data", notifying customers within 72 hours of a data breach, upholding consumers' right to know whether, where and why their data is being processed, and providing users with tools to download or delete their data.[65] Representative Marsha Blackburn (R-Tenn.), chair of the House Committee on Energy and Commerce's Subcommittee on Communications and Technology, has proposed the Balancing the Rights of Web Surfers Equally and Responsibly (BROWSER) Act. Similar to the CONSENT Act, this legislation would require Internet service providers and platforms like FB to receive opt-in approval for information about "a person's health, financial information, web browsing history, location, or information about children under 13."[66] One proposed law that FB has endorsed, and is preemptively implementing, is the Honest Ads Act, which would "require tech companies with more than 50 million monthly users to maintain a public file of all political ads purchased by anyone spending more than $500."[67] What Congress will do is still unclear, subject to industry lobbying efforts and the evolution of public attitudes over time.

Human Capital, by Marika Zadva, Department of State

In today's world, the gap between the countries that lead the technology field is closing and the U.S. now finds itself competing with China, India, South Korea, and others who have invested in their own tech industries and prioritized STEM education to create skilled workforces.

In order for the U.S. to succeed in the future and compete with these countries, the solution must be for government and industry to work closer together, to build trust, and to help each other achieve national goals of security and prosperity. What is needed are steady government policies that allow for a stable education and workforce development process. A number of programs are already in place,[68] but these programs must be expanded and reinforced; the goal must be to improve the quality of and increase the number of S&E graduates so that tech firms can rely on qualified U.S. workers for their needs. Consistent policies and steady funding for programs are keys to their success as these programs take years of effort in order to show results and changes to policy and funding only disrupt their effectiveness and provoke failure; continuing resolutions and government shutdowns do not provide the stability needed. The programs must be at all levels, from K-12 through university to adult learning and job retraining, especially as technology eliminates traditional jobs at an ever-faster pace.

Congress has a key role to play in this. Bills such as the Strengthening Career and Technical Education for the 21st Century Act, the Championing Apprenticeships for New Careers and Employees in Technology (CHANCE in Tech) Act, and the Higher Education Act are important for ensuring coordinated strategy and committed focus by the government on behalf of students nationwide; unfortunately, these bills as well as many others have been

languishing in committee for months and years with little action.[69] Threats to graduate students who faced tax increases as their waived tuition fees were targeted as taxable income during the recent tax reform debates result in discouraging students from pursuing higher education, when the opposite is needed. Instead, policies are required that make it easier for students to obtain quality education without being burdened by crushing debt.[70]

Until now, policy has been unable to reconcile the issue of off-shoring and guest workers and the fact that American S&E graduates are taking jobs in other occupations because they can find better job offers and opportunities.[71] The problem may not be the lack of qualified U.S. workers, but the lack of appropriate pay or benefits to attract qualified U.S. workers. While empirical studies show that there are enough qualified U.S. workers, they are choosing jobs outside their field of study, such as in health care and finance, due to better pay and benefits.[72] Solutions must be found, like revising the H1-B visa program to mandate employers to show proof that they tried to hire U.S. workers (which despite common belief to the contrary is not currently required) in order to advantage U.S. workers and provide attractive career paths in the science, technology and engineering fields for those students that have invested the time and money to pursue a STEM education. If there really were a shortage of U.S. workers, the market should adjust by increasing wages, which hasn't happened in any meaningful way.[73]

Signs are positive that the U.S. is on the right track for addressing the nation's human capital needs in the ICT sector. However, without close collaboration between government, academia, and ICT firms, the U.S. will not be able to compete with countries that dedicate their full resources to competing and winning the race for technological supremacy. It is essential that good communication be established and trust built among all sides, so that efforts can be combined and all can work toward the same goals. Unless the U.S. can unite all actors who are responsible for ensuring that the U.S. remains a leader in innovation and technology, it will find itself falling behind foreign competitors.

Policy Recommendations:

- Ensure stable funding and consistent policies for education and workforce development focused on K-12 through university as well as adult learning and job retraining; and
- Require that employers document attempts to hire U.S. workers before qualifying for H-1B visas.

The ICT Sector and the Defense Acquisition System, by Mark Harrington, Department of Homeland Security, and Lt. Col. Emmanuel Thome, French Defense Procurement Agency (DGA)

The ICT sector and the DoD enjoy a strong relationship; advances in ICT benefit development in military operations and vice versa. ICT has changed the ways the military operates; it has constituted a decisive driver to enhance land, sea, air, and space operations, and is now gaining an even larger role as a game changer in future operations in a fifth domain (cyberspace). ICT is a field in which research, technology development, and manufacturing can be used for both military and civil applications. Given the large amount of investment done by the private sector, it is in the interest of national security to be sufficiently agile to benefit from technologies developed and funded by the ICT community. ICT is also the world's leading ecosystem of technological innovation as Silicon Valley symbolizes a new state of mind, exploiting innovation in every sector, including national security. To retain its technological

edge, the U.S. military needs to embrace this Silicon Valley spirit, exploiting components and systems arguably more advanced in most critical areas than the technologies produced by the traditional defense-industrial base (DIB).[74]

ICT creates millions of jobs, and serves as a strong driver for innovation, research, and development. ICT is said to have accounted for more than 25% of U.S. economic growth from 1995 to 2009.[75] The defense and government acquisition processes have been slower to embrace its many benefits and rapid evolution.

Innovation must be quick in the ICT community, but it hits a wall in the defense acquisition world. Although our acquisition system is intended to be fair, open and orderly, it is slow, burdensome, expensive, and difficult. "The current bureaucratic approach, centered on exacting thoroughness and minimizing risk and [is]… increasingly unresponsive. We must transition to a culture of performance where results and accountability matter."[76] "Often, it's about whether the jurisdiction has met the procurement laws first, and perhaps secondly whether or not they actually achieved the outcomes they were looking for."[77] Additionally, we have concentrated on cost and performance while accepting a slow time schedule. In the innovation world, we must orient around the paradigm and metric of time.

Additionally, a House Armed Services Committee panel found that a "number of hurdles make it challenging for companies to compete for defense contracts. The plethora of regulations dissuades many companies from competing for government contracts.[78] It takes time to learn the many regulations; therefore, the high rate of turnover in government acquisition personnel affects the quality and consistency of policies…and lacks "consistently trained, skilled personnel."[79]

Other acquisition hurdles include: lack of industry understanding of the government process, reliance on personal connections, contract "vehicles" that limit competition based on past performance ratings on previous government contracts, limiting qualifications to "favored" company classifications, limited potential, a lack of transparency, and IP concerns of security and secrecy. Additionally, poorly articulated requirements and a lack of iterative feedback in the development process inhibits progress or better solutions; the two thousand pages of the (Defense) Federal Acquisition Regulation (DFAR/FAR) add years to projects. Add the rapid evolution of technology to a slow, inflexible and expensive bureaucratic process to the alignment of technology and procurement and you have a lot of tension. Thus, DoD acquisition policies and processes provide little incentive for the defense industry to invest in innovation.[80]

Leveraging ICT strengths constitutes a real opportunity for DoD to access cutting-edge technologies that give a decisive competitive advantage to the U.S., but this will require a new state of mind in the defense acquisition system. More innovative military equipment at lower cost will require DoD to lower barriers to entry in order to enlarge competition, diversity, and innovation within the defense contractors. The use of Defense Innovation Unit Experimental (DIUx), Other Transaction (OT) contracting, venture capital, tradeoff process instead of lowest price/technically acceptable (LPTA), and generally more agile practices in the Pentagon are available tools to take up future national security challenges.

Policy Recommendations:

- Create a *National Innovation Center* that gathers a voluntary repository of information on innovation projects in universities, government, private, and public companies;
- Close the gap between DoD "end users" and startups looking for investments could be closed through the creation of a venture capital office based on the successful In-Q-Tel

model in the U.S. intelligence community; and

- Expand the use of OT authority beyond R&D or prototyping work to increase innovation in major defense acquisition programs, bring more flexibility into defense contracts, and lower barriers of entry.

Cybersecurity, by Ken Graf, U.S. Secret Service,
Maura Styczynski, Department of the Navy, and Col. Jaak Tarien, Estonian Air Force

Research agency Gartner Data predicts that "60% of digital businesses will suffer service failures as a result of IT security issues by 2020."[81] It has been more than a decade since the first nation-on-nation cyberattack; yet, although cyberattacks on government infrastructure and private industry have become almost a routine occurrence, both the public and private sectors are slow to make significant improvements in their cybersecurity posture, with some observing that the lack of a profitable business case for proper cybersecurity is to blame.[82] In the absence of market demand, companies have largely failed to invest in more robust and effective countermeasures, or adopt practices of continuous, vigilant improvement. Government policy in the U.S. has also been traditionally modest, allowing market forces to rectify the issue rather than instituting policies that foster a secure cyber environment. Although some essential policies have been adopted to force the DIB to implement more robust cybersecurity measures, both government and industry remain behind the curve.

Recent cyber breaches have had limited economic impact to the companies affected.[83] Shareholders simply do not possess sufficient information or knowledge to measure the impact of an incident.[84] The public sees cyberattacks and hacking as inevitable. Companies hit by cyberattacks are viewed as victims, not as co-culprits due to negligence. Largely due to this dismissive public attitude, even existing security standards are not being implemented. For example, in the Target breach of 2013, when the personal data of millions of customers was stolen, the company was not adhering to the Payment Card Industry (PCI) Data Security Standard (DSS). Yet, Target's share price dropped by a mere 0.3% and recovered quickly.[85]

The DIB faces larger challenges than other industries. In addition to activist hacking and cybercrime, the DIB faces the escalated interest of government-backed hacking. Dr. Tom Kennedy, Chairman and CEO of the Raytheon Company and Vice Chairman of the Aerospace Industries Association, recently noted, "aerospace and defense organizations are continuously attacked by increasingly sophisticated parties who themselves leverage tools like cloud computing and viruses to increase the scale and impact of their activities."[86]

It is essential for the national security system to re-examine policies, regulations, and system architectures for cybersecurity. Government regulation needs to support an adaptive online environment, imposing an obligation to constantly monitor threats and adopt a preemptive posture. Today, the DIB is subject to FedRAMP to standardize cyber monitoring for cloud products and services. The Defense Federal Acquisition Regulation Supplement (DFARS) also mandates that defense contractors adhere to cybersecurity guidelines in order to maintain contracts on government security projects. Both FedRAMP and DFARS requirements are fairly new and have yet to be fully adopted.

Outside of government, minimal regulation exists, even in industries designated by the DHS as "critical infrastructure." The federal government's current posture is set forth in Presidential Policy Directive-21 (PPD-21, February 2013), which named DHS as the responsible federal agency for coordinating "the overall Federal effort to promote the security

and resilience of the Nation's critical infrastructure."[87] PPD-21 identified 16 sectors whose "systems and assets, whether physical or virtual, [are] so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[88] Within DHS, the NCCIC acts as an intermediary between federal cybersecurity centers and the private sector, utilizing fusion centers and Information Sharing and Analysis Centers (ISACs). Participation is strictly voluntary for the private sector, however, and varies widely across industries. Policymakers need to arm the NCCIC with the statutory/regulatory authority to ensure effective cybersecurity practices within all critical infrastructure, and to inspect/audit networks to ensure compliance. Additionally, policymakers should re-evaluate what industries and corporations should be included within the 16 sectors.

More broadly, if we are to overturn the attackers' advantage, we first need to adopt a robust, yet agile and adaptive, cybersecurity posture across government, and create economic incentives for private industry to do the same. One nascent technological response that may have the opportunity to support a robust posture for the most sensitive public and private data is blockchain. While some benefits of the decentralized Internet are its speed, openness, and lack of friction, these are accompanied by reciprocal costs to security. Blockchain technology may provide an answer to data protection and integrity issues.

Blockchains are records of cryptographically-linked data built on a distributed network. Although distributed systems have been popularized through the bubble-like rise of cryptocurrencies like bitcoin and ethereum, blockchain use cases abound in more areas than just Financial Technology (FinTech) and meet the standards set by the NIST for cybersecurity: confidentiality, integrity, and availability.[89] The *confidentiality* of data in the blockchain is maintained with encrypted data-in-transit. Some existing commercial blockchains even apply post-quantum cryptography to ensure that data will still be protected when quantum computing makes RSA-based encryption obsolete. The immutability and traceability that form the backbone of blockchain assure the network *integrity*.[90] Sequential hashing and cryptography, in combination with network distribution, make tampering with data extraordinarily challenging. Non-repudiation is guaranteed because every transaction in blockchain networks is cryptographically associated with each user. Data *availability* in the blockchain is inherent in the distributed nature of the technology as well.[91] If one node of the network is disrupted, every other node is still fully functional; there is no single point of failure.

Whether it is increased regulation, financial accountability, or system architecture overhauls, the government must respond to the increasing threat from state and non-state cyber criminals or suffer the consequences to our national security.

Policy Recommendations:

- Establish a committee within USCYBERCOM to identify opportunities for using distributed systems to transact with critical data;
- Take leadership in forming a dedicated alliance of free and democratic nations to deter and defend against cyber attacks on our democratic societies; and
- Establish legislative and regulatory requirements to mandate industry cooperation with DHS/NCCIC, and to hold industry executives liable for cyber incidents that result from negligence in implementing known best practices.

Privacy, Security, and Oversight, by Paul Fritch, Department of State, Col. Amado Sanchez, USA, Lt. Col. Paul Sebold, USAF, and Lt. Col. Ryan Vetter, USAF

In today's competitive environment, information is a commodity essential to business relevancy. Government needs to ensure access to information, just as the interstate highway system and public transportation connect people to business. Simple access to the Internet is no longer enough, with connection speeds[92] and content quality now subjects for debate in the halls of Congress.

Advances in digital technology have also provided citizens with remarkable tools for staying informed and organizing. They have been a boon to law enforcement and intelligence collection, allowing local, state, and federal government officials to track, infiltrate, and disrupt a wide range of criminal and terrorist activities. At the same time, development of these technologies has outpaced the evolution of a legal framework sufficient to guarantee respect for Constitutional liberties, leaving it largely to the courts to sort out how to protect Americans from unreasonable searches and seizures in an age when most citizens willingly carry a highly capable digital tracking device on their person 24 hours a day, and the "Internet of Things" is spreading networked sensors throughout their homes.

While Americans have bristled at the notion that their government might surveil them online, they have voluntarily surrendered a wealth of personal data to large tech companies in exchange for convenience and functionality. This has enabled hostile foreign intelligence services to exacerbate and exploit societal tensions and pre-existing political polarization in ways that risk undermining the integrity of democratic institutions (particularly if executed in conjunction with other "hybrid" tactics, such as "doxing" of public figures and/or hacking of voter registration lists or voting systems). If the debate over government's role in monitoring the digital world stems from an inherent tension *between* privacy and security, in the private sector the voluntary surrender of privacy *creates* a potential national security threat. The Seminar's work coincided with a number of high-profile debates over data privacy and national security, including indictment by the DoJ Special Counsel of Russian individuals and entities seeking to influence the 2016 Presidential election, the Facebook/Cambridge Analytica scandal, and a wide range of international initiatives to promote data privacy and enable government surveillance. Government regulation and oversight of social media is important to national security due to their ability to influence large segments of the U.S. and global populations.

Addressing the disparate challenges posed by compromised privacy in the digital world will require concerted, thoughtful action by government and industry. In the short term, industry is in a stronger position to act in response to market forces, while Congress and the executive branch struggle both to understand rapidly evolving technologies and to resolve conflicting public interests. Constitutionally-based government oversight linked to the protection of individual rights, free speech, and privacy should provide government with the mandate to ensure firms like Facebook, Google, and Twitter are prioritizing the interests of their customers. Additionally, government should provide basic consumer protections by ensuring social media user agreements are easy to understand and do not infringe on individual rights. Ultimately, enhanced *clarity* and *transparency* can enhance both civil liberties and confidence in industry and governmental institutions.

Taking swift, effective action on data privacy can also help ensure that the U.S. retains its global leadership in ICT governance, as international norms of conduct begin to diverge. U.S.

ICT firms seeking to operate in international markets are subject to rules and regulations of other countries, while remaining exposed to U.S. policy decisions and their potential fallout.[93] The problem increases for tech companies whose profitability relies upon detailed personal and private information, which may be targets of government surveillance.[94] High-profile breaches of personal data have resulted in a wide range of new laws for data localization and protection. The EU, Brazil, China, Russia, and Iceland have adopted localization requirements, forcing firms to navigate confusing and contradictory regulations.[95] At one end of the spectrum, U.S. firms remain accountable under strict data privacy protections, such as the EU's GDPR. At the other, they (and their American clients) remain vulnerable to state surveillance in countries like Russia and China. China in particular, empowered by indigenous tech giants Alibaba and TenCent, is leveraging its success in ICT innovation in order to enhance social and political control over its populace, and could export its growing expertise in tech-enabled social engineering.[96]

In Xinjiang Province, home of the Uighur minority, China has built the world's most thorough electronic surveillance apparatus.[97] Residents of Xinjiang are tracked constantly by facial recognition systems, license plate readers, CCTV, "convenience police stations," ID card scanners, and USB sensors to check phones for unapproved software applications.[98] Elsewhere across the PRC, the ubiquitous adoption of "super apps" such as Alipay and WeChat has funneled the majority of social, travel, and economic activity from urban Chinese citizens through a duopoly of state-accessible, information collection points.[99] These apps function as a combination of social media, communications, navigation, shopping, banking, and mobile payment; relying on the wide prevalence of QR codes in Chinese society to link physical objects in the real world to the internet user experience.[100] In many places, cash is no longer a payment option, forcing residents into the WeChat/Alipay ecosystem. Alipay and WeChat launched credit rating systems in 2013, challenging users to treat their personal reliability scores like a game, offering discounts and special offers to those with good credit. Unreliable behavior decreases one's credit, and so does having friends with low credit scores.[101] The emergence of these "government controlled" social media applications complicates U.S. efforts to allow companies to self-regulate while setting international standards for acceptable levels of privacy and protection for consumers.

China's advances in facial recognition, smart city monitoring, the IoT, and personal social credit scores are likely to spread to nations looking to gain additional security at the expense of personal liberty. Where this expansion is accompanied by Chinese investment and technology, then the nations adopting the systems will also be opening the door to exploitation by the Chinese military and economic intelligence apparatus. In this context, enhanced cooperation with the EU and other like-minded countries to shape international norms is imperative for continued economic growth and sustained U.S. leadership in the ICT industry.

Policy Recommendations:

- Codify digital Fourth Amendment protections in a "Digital Bill of Rights," to include regulation of IoT sensors, such as microphones and videocameras, and informed consent standards with regard to emerging technologies such as facial recognition;
- Enact "right to know" legislation, requiring digital advertising platforms to notify users when their data has been shared with third parties, and for what purpose, and reconsideration of the March 2017 repeal of FCC regulations that had prevented telecommunications providers from tracking users' browsing history without permission;[102] extend existing

regulation of broadcast political advertising to online platforms, requiring transparency with regard to sources and funding (Facebook recently announced that it would take this step unilaterally[103], but such a step should be enacted into law and policed by the Federal Election Commission);

- Work with allies (particularly in the EU) on the development of generally accepted international standards for data privacy;
- Raise awareness of U.S. firms of the ethical and security implications of doing business inside China or working with Chinese ICT firms on critical infrastructure initiatives; use regulatory tools (e.g., CFIUS) to discourage American companies from participating in joint ventures with Chinese firms where the likelihood of misuse of technology (or user data) is high; and
- Closely track the development of Chinese surveillance and big data innovations that might have the potential to migrate beyond Chinese society; discourage (and possibly legislate against) the establishment in the U.S. of non-voluntary credit scoring apps that rely on social media or mobile payment information, especially data obtained through "friend-of-a-friend" type third party sourcing.

Conclusion

Information and communications technology (ICT) is perhaps the most complex and dynamic of the 20 industries studied by the Eisenhower School in 2018. Beyond its direct impact as a driver of innovation, growth, and job creation, it has become an essential enabler of virtually every sector of the economy, including the day-to-day operations of government. Retaining U.S. leadership in the sector will require a sustained, multi-pronged effort. While the U.S. remains the global leader in the ICT field, it now faces intense competition from countries such as China, India, and South Korea, among others. Policymakers must focus on optimizing collaboration between public and private sectors to address national security needs while fostering the entrepreneurial and innovative environment that has allowed the ICT sector to thrive and lead globally. Without close collaboration among all sides, the U.S. will not be able to compete with countries who dedicate their full resources to winning the race for technological supremacy. Challenges that must be addressed include:

- Fostering conditions that encourage innovation and growth, including through the development of sufficient human capital;
- Adapting federal acquisition processes to better leverage technological innovation in ICT;
- Anticipating, deterring, and preventing threats to critical infrastructure, government operations, and commercial activity in cyberspace; and
- Ensuring that regulation keeps pace with technological development, in a manner that ensures both national security and the protection of individual rights.

NOTES

[1] *Mobile Fact Sheet*, Pew Research Center, Internet & Technology, February 5, 2018, http://www.pewinternet.org/fact-sheet/mobile/.

[2] "IT Industry Outlook 2018", Computer Technology Industry Association (CompTIA) 2018. https://www.comptia.org/resources/it-industry-trends-analysis.

[3] Ibid.

[4] Source: Statista.com (https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-value/).

[5] "IT Industry Outlook 2018", Computer Technology Industry Association (CompTIA) 2018. https://www.comptia.org/resources/it-industry-trends-analysis.

[6] Information and communication technology (ICT) research and development (R&D) expenditure in the United States and worldwide, from 2015 to 2018 (in billion U.S. dollars), 2018, accessed March 27, 2018, https://www.statista.com/statistics/732308/worldwide-research-and-development-information-communication-technology/.

[7] Greg Ip, "The Antitrust Case Against Facebook, Google and Amazon, A few technology giants dominate their worlds just as Standard Oil and AT&T once did. Should they be broken up?", *Wall Street Journal*, January 16, 2018, accessed April 15, 2018, https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561..

[8] Jacob Poushter, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies, But advanced economies still have higher rates of technology use," Pew Research Center Global Attitudes and Trends, February 22, 2016, http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/, 16.

[9] David Goldman, "What is 5G?," CNN Tech (blog), January 29, 2018, http://money.cnn.com/2018/01/29/technology/what-is-5g/index.html.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Marguerite Reardon, "Trump's Crazy 5G Plan Actually 'Diagnoses a Real Problem*"* CNET (blog), January 30, 2018, https://www.cnet.com/news/trumps-crazy-5g-plan-diagnoses-real-problem-cybersecurity-threat/.

[14] Linda K. Moore, *Framing Spectrum Policy: Legislative Initiatives.* CRS Report No. R44433 (Washington, DC: Congressional Research Service, 2016), https://fas.org/sgp/crs/misc/R44433.pdf, 1.

[15] Thomas K. Sawanobori and Dr. Robert Roche, *From Disposal to Deployment: The History of Spectrum Allocation Timelines,* https://api.ctia.org/docs/default-source/default-document-library/072015-spectrum-timelines-white-paper.pdf, 1.

[16] White House, *National Security Strategy of the United States of America*, December 2017, 3.

[17] Steve Lohr, "How Big Data Became So Big." www.newyorktimes.com, August 11, 2012, accessed April 11, 2018, https://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html?_r=0..

[18] Saul Judah and Ted Friedman, *The State of Data Quality: Current Practices and Evolving Trends,* Technical paper no. G00255625. Stamford, CT: Gartner, 2013, 2.

[19] "P-Tech: when ambition meets opportunity, success happens," IBM, accessed April 12, 2018, https://www.ibm.com/thought-leadership/ptech/index.html.

[20] Michael S. Teitelbaum, *Falling Behind?: Boom, Bust, and the Global Race for Scientific Talent* (New Jersey: Princeton University Press, 2014), 208.

[21] Ibid, 133.

[22] Jason Tama, "There's no app for that: disrupting the military-industrial complex," Center for 21st Century Security and Intelligence, July 2015, accessed April 6, 2018.

[23] Ibid.

[24] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Maryland, 2004), https://library.bowdoin.edu/research/chicago-gov.pdf, 2.

[25] Section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, available at http://www.gpo.gov/fdsys/pkg/BILLS-111hr6523enr/pdf/BILLS-111hr6523enr.pdf. Axelrod, C. Warren, "Mitigating Software Supply Chain Risk," ISACA JOnline, August, 2013, , accessed May 6, 2018, http://www.isaca.org/Journal/archives/2013/Volume-4/Pages/JOnline-Mitigating-Software-Supply-Chain-Risk.aspx.

[26] Adam Jourdan, "U.S. strike on China's ZTE another blow for Qualcomm," April 17, 2018, accessed May 7, 2018, https://www.reuters.com/article/us-china-zte-qualcomm-analysis/u-s-strike-on-chinas-zte-another-blow-for-qualcomm-idUSKBN1HO0XT..

[27] "CFIUS intervenes in Broadcom's attempt to buy Qualcomm," *Economist*, March 8, 2018, accessed May 7, 2018, https://www.economist.com/news/business/21738398-powerful-committee-top-american-officials-becomes-more-intrusive-cfius-intervenes.

[28] Paul Mozur, "The World's Biggest Tech Companies Are No Longer Just American," *New York Times,* August 17, 2017,accessed April 1, 2018, https://www.nytimes.com/2017/08/17/business/dealbook/alibaba-sales-revenue-first-quarter-profit.html.

[29] Dune Lawrence and Lulu Chen, "The People's Republic of WeChat," *Bloomberg Businessweek* no. 4479 (June 13, 2016), 64-66.

[30] Everett Rogers, *Diffusion of Innovations: Fifth Edition*. (Free Press, New York, 2003), 434.

[31] Ibid.

[32] Ibid.

[33] Ibid.

[34] Ibid., 229.

[35] Ibid., 240.

[36] Ibid., 257.

[37] Ibid., 258.

[38] Ibid., 258.

[39] Collin Gray, *Recognizing and Understanding Revolutionary Change in Warfare,* (Carlisle Barracks, Strategic Studies Institute, 2006), 11.

[40] Department of Defense, Summary of the 2018 National Defense Strategy of the United States of America, 2018, 10.

[41] Linda K. Moore, "Framing Spectrum Policy: Legislative Initiatives," CRS Report No. R44433 (Washington, DC: Congressional Research Service, 2016), https://fas.org/sgp/crs/misc/R44433.pdf, 1.

[42] Moore, Summary.

[43] Sawanobori and Roche, 2.

[44] Ibid., 3-7.

[45] Ashton B. Carter, "DoD Electromagnetic Spectrum Strategy" (Washington, DC: Pentagon, 2013), http://dodcio.defense.gov/Portals/0/Documents/Spectrum/Electromagnetic%20Spectrum%20Strategy%20(Glossy).pdf, 1.

[46] Sawanobori and Roche, 1.

[47] Michael O'Rielly, "How to Free Up Government Held Spectrum in the Face of Increasing Budgetary Pressure," Federal Communications Commission (blog), September 6, 2017, https://www.fcc.gov/news-events/blog/2017/09/06/how-free-government-held-spectrum-face-increasing-budgetary-pressure.

[48] Carter, 1.

[49] Ibid.

[50] O'Rielly.

[51] Discussion During a Seminar Meeting with a Trade Association, (group discussion, Washington, DC, February 21, 2018).

[52] Discussion in Seminar Room, (group discussion, Ft. McNair, Washinton, DC, January 26, 2018).

[53] Jonathan R. Agre and Karen D. Gordon, *A Summary of Recent Federal Government Activities to Promote Spectrum Sharing,* IDA Paper P-5186, accessed on April 13, 2018 (Washington, DC: Science and Technology Policy Institute, 2015), https://www.ida.org/STPI/ExploreSTPIResearch/STPIPublications, viii.

[54] Mark D. Ryan, "Cloud Computing Privacy Concerns on Our Doorstep." ACM. January 01, 2011, accessed April 13, 2018, https://cacm.acm.org/magazines/2011/1/103200-cloud-computing-privacy-concerns-on-our-doorstep/fulltext.

[55] GSA, Federal Acquisition Service, GSA.GOV, accessed April 12, 2018, https://www.gsa.gov/cdnstatic/Best_Business_Practices_for_US_Government_Cloud_Adoption.pdf.

[56] Lohr.

[57] Jerry Staple, "Big Data and The Fourth Industrial Revolution," *Origin Digital*, August 24, 2017, accessed April 12, 2018, http://www.origin-digital.com/big-data-fourth-industrial-revolution/.

[58] Bernard Marr, "Why Everyone Must Get Ready for the 4th Industrial Revolution," Forbes.com, April 5, 2016, accessed April 12, 2018, https://www.forbes.com/sites/bernardmarr/2016/04/05/why-everyone-must-get-ready-for-4th-industrial-revolution/#137bd493f90b.

[59] Klaus Schwab, *The Fourth Industrial Revolution, What It Means and How to Respond*, (New York: Crown Business, 2017), 9.

[60] Ibid.

[61] Judah and Friedman, 2.

[62] Craig Timberg and Tony Romm. "Facebook CEO Mark Zuckerberg to Capitol Hill: 'It Was My Mistake, and I'm Sorry.'" MSN.com, April 9, 2018, accessed April 9, 2018, https://www.msn.com/en-us/news/politics/facebook-ceo-mark-zuckerberg-to-capitol-hill-'it-was-my-mistake-and-i'm-sorry'/ar-AAvGddk?ocid=spartandhp.

[63] Khari Johnson, "5 Ways Congress Could Regulate Facebook." *VentureBeat*, April 14, 2018, accessed April 15, 2018, https://venturebeat.com/2018/04/14/5-ways-congress-could-regulate-facebook/.

[64] Marguerite Reardon, "Senate Dems Introduce 'privacy Bill of Rights'," *CNET*, April 10, 2018, accessed April 15, 2018, https://www.cnet.com/news/senate-dems-introduce-privacy-bill-of-rights/.

[65] Johnson.

[66] James Cooper, "The BROWSER Act: A Worthy Goal, But There's an Easier Fix to the Net Neutrality Privacy Mess." *Forbes*, May 26, 2017, accessed April 15, 2018, https://www.forbes.com/sites/jamesccooper1/2017/05/26/the-browser-act-a-worthy-goal-but-theres-an-easier-fix-to-the-net-neutrality-privacy-mess/#20469ebcea19.

[67] Ibid.

[68] Examples of programs include the U.S. Department of Labor's registered apprenticeship program managed by the Office of Apprenticeship, the CyberCorps Scholarship for Service program co-sponsored by the Department of Homeland Security and the Office of Personnel Management but hosted by the National Science Foundation, and the Computer Science for All Initiative, which aims to expand computer science education across all states by providing funding, teacher training, access to instructional materials, and regional partnerships. See U.S. Department of Labor, "Frequently Asked Questions about the Apprenticeship Program", accessed March 19, 2018, https://www.dol.gov/featured/apprenticeship/faqs; NICE National Initiative for Cybersecurity Education brochure, accessed March 19, 2018, https://www.nist.gov/itl/applied-cybersecurity/nice/about; The White House, *FACT SHEET: President Obama Announces Computer Science for All Initiative*, Office of the Press Secretary, January 30, 2016, accessed March 29, 2018, https://obamawhitehouse.archives.gov/the-press-office/2016/01/30/fact-sheet-president-obama-announces-computer-science-all-initiative-0.

[69] The website www.Congress.gov provides the status of bills pending with the current Congress as well as with past Congresses.

[70] Erica L. Green, "Graduate Students Escaped Tax Increases, but They still Feel a Target on Their Backs," *New York Times*, December 19, 2018, accessed March 19, 2018, https://www.nytimes.com/2017/12/19/us/politics/graduate-students-education-tax-bill.html.

[71] Teitelbaum, 132.

[72] Ibid, 126-127.

[73] Hal Salzman, "What Shortages? The Real Evidence About the STEM Workforce." *Issues In Science & Technology* 29, no. 4: 58-67 (Summer 2013): 64, accessed April 12, 2018, Academic Search Premier, EBSCOhost..

[74] Adam Jay Harrison, "DOD 2.0: High Tech Is Eating the Pentagon," *U.S. Naval Institute Proceedings* 142, no. 2: 60-65 (2016), accessed March 19, 2018, Academic Search Premier, EBSCOhost,.

[75] Ezell and Andes, 75.

[76] 2018 National Defense Strategy, 10.

[77] Justin Brown, "Bringing Innovation to Procurement," GovTech.com, March 22, 2018, accessed on April 5, 2018, http://www.govtech.com/budget-finance/Bringing-Innovation-to-Procurement.html..

[78] House Committee on Armed Services, Challenges to Doing Business with the Department of Defense: Findings of the Panel on Business Challenges in the Defense Industry, March 19, 2012, accessed April 4, 2018, https://wcoeusa.org/sites/default/files/Challenges%20to%20Bus%20with%20DOD.3.12.pdf..

[79] Ibid.

[80] Ibid.

[81] Nick Ismail, "Cyber security – the unrelenting challenge for leadership," Information Age, September 7, 2017, accessed April 9, 2018, http://www.information-age.com/cyber-security-unrelenting-challenge-leadership-123468401/..

[82] Email interview with a high level Cybersecurity Policy staff member at NATO HQ, Brussels, Belgium. Conducted 16-18 March 2018 by Jaak Tarien, Estonian Air Force.

[83] Elena Kvochko and Rajiv Pant, "Why Data Breaches Don't Hurt Stock Prices," *Harvard Business Review*, March 31, 2015, accessed April 7, 2018, https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices.

[84] Ibid.

[85] Peter Purcell, "What the board needs to know about cybersecurity compliance," CIO, January 19, 2018, accessed April 9, 2018, https://www.cio.com/article/3023865/cyber-attacks-espionage/what-the-board-needs-to-know-about-cybersecurity-compliance.html.

[86] Kathryn Verona, "Cyber Security and the Aerospace and Defense Industry. Challenges, Issues and Solutions," Aerospace Industries Association. September 13, 2017, accessed April 9, 2018, https://www.aia-aerospace.org/cyber-security-and-the-aerospace-and-defense-industry-challenges-issues-and-solutions/.

[87] White House, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," Office of the Press Secretary, February 12, 2013, accessed March 24, 2018, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[88] Ibid.

[89] U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards Publication 199 (Maryland, 2004), https://library.bowdoin.edu/research/chicago-gov.pdf, 2.

[90] Eric Piscini, David Dalton, and Lory Kehoe, *Blockchain & Cyber Security Point of View*, (Deloitte, April 2017), 7.

[91] Ibid, 10.

[92] Robert McMillan, "What Everyone Gets Wrong in the Debate Over Net Neutrality," *Wired Business*, June 23, 2014, accessed April 8, 2018, https://www.wired.com/2014/06/net-neutrality-missing/, 1.

[93] Henry Farrell and Abraham Newman, "The Transatlantic Data War," *Foreign Affairs* 95, no. 1 (Jan, 2016), 128.

[94] Ibid.

[95] Christopher Smart, *Regulating the Data that Drive 21st-Century Economic Growth - the Looming Transatlantic Battle,* Chatham House: The Royal Institute of International Affairs, (2017), 7.

[96] Mozur.

[97] Josh Chin, and Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *Wall Street Journal,* December 19, 2017, accessed April 1, 2018, https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.

[98] Ibid.

[99] Lawrence and Chen, 64-66.

[100] Mozur.

[101] Mara Hvistendahl, "Inside China's Vast New Experiment in Social Ranking," *Wired Magazine*, December 14, 2017, accessed April 1, 2018, https://www.wired.com/story/age-of-social-credit/.

[102] Cecilia Kang, "Congress Moves to Strike Internet Privacy Rules From Obama Era," *New York Times*, March 23, 2017, accessed April 1, 2018, https://www.nytimes.com/2017/03/23/technology/congress-moves-to-strike-internet-privacy-rules-from-obama-era.html?mtrref=www.nytimes.com.

[103] Jack Nicas, "Facebook to Require Verified Identities for Future Political Ads," *New York Times*, April 6, 2018, accessed April 1, 2018, https://www.nytimes.com/2018/04/06/business/facebook-verification-ads.html.