Spring 2019

Industry Study

Final Report

Cyber Domain and Advanced Computing

13

The Dwight D. Eisenhower School for National Security and Resource Strategy

National Defense University

Fort McNair, Washington D.C. 20319-5062

CYBER DOMAIN AND ADVANCED COMPUTING 2019

Table of Contents

ABSTRACT: The United States is in a great power competition that is increasingly fueled by an information revolution within the ever-evolving cyber domain. To enable future leaders and policy-makers to prevail in this domain, the Eisenhower School's Cyber Domain / Advanced Computing Industry Study (IS) examined key information technologies (IT), including artificial intelligence (AI), blockchain, commercial cloud, and quantum computing. The U.S. Government should increase its partnerships with academia and private industry as a triple helix of intertwined equities and investments. Doing so will stimulate economic growth, address threats, and develop human capital. U.S. leadership is needed to encourage and enact effective cyber legislation and policies to protect citizens. Such a strategic approach enables development of a cyber-savvy culture and society capable of nurturing international cyber norms and fostering global cooperation.

Students and Faculty

Lt Col Matthew Belle	United States Air Force
Col Shlomi Binder	Israeli Defense Forces
CDR Derrick Blackston	United States Navy
Mr. Anthony Burke	National Security Agency
CDR Ahmed Al-Busaidi	Royal Oman Navy
Mr. Michael Cirillo	United States Marine Corps
COLPatrick Curry	United States Army
COLJacquelin Emmanuel	United States Army
LtCol Paul Gillikin	United States Marine Corps
BGen Shamshudin Kassim	Royal Malaysian Air Force
LTC Edward Kendall	United States Army
Ms. Allison Lee	Department of State
COL Edward Meyers	United States Army
Lt Col Ty Miller	United States Air Force
Mr. Ric Nordgren	Defense Acquisition University
Col Suleyman Ugural	Turkish Army
Mr. David Vargas	Defense Intelligence Agency

Col Andrew Nichols	United States Air Force Reserve, Primary Faculty Lead
Mr. Steve Bloor, J.D.	National Security Agency, Co-Lead
Col (R) Brian Buckles	Eisenhower School
COL Sharon McBride	United States Army
Mr. David White	Eisenhower School

Industry Study Outreach and Field Studies

On-campus Presenters

United States (U.S.) Cyber Command (USCYBERCOM), Fort Meade, MD
CyberSponse, Arlington, VA
Illumio, Sunnyvale, CA
University of Maryland, Quantum Computing and Neuromorphic Computing, MD
Enlighten IT Consulting, Linthicum Heights, MD
Amazon Web Services, Herndon, VA
Defense Security Service, Washington DC
North Atlantic Treaty Organization (NATO), Allied Command Transformation, Norfolk, VA
Office of the Under Secretary of Defense (OUSD) for Intelligence, Intelligence / Surveillance / Reconnaissance, Warfighter Support, Washington DC
National Security Agency (NSA), Ft. Meade, MD
U.S. Patent and Trademark Office, Alexandria, VA
OUSD for Acquisition and Sustainment, Washington DC
J Capital Research, Hong Kong and New York, NY
Eaton Vance, Boston, MA
Microsoft, Arlington, VA
U.S. House of Representatives, Washington, DC

Field Studies – Domestic

Air Force Office of Special Investigations, Joint Base Andrews, MD
Federal Bureau of Investigations, Quantico, VA
Cyber Threat Alliance, Arlington, VA
Business Software Alliance, Arlington VA
USCYBERCOM, Ft. Meade, VA
Carnegie Mellon University, Pittsburg, PA
National Cyber-Forensics and Training Alliance, Pittsburg, PA
Verizon, Ashburn, VA
Department of Homeland Security, Arlington, VA
Northrop Grumman, Annapolis Junction, MD
University of Maryland Laboratory for Telecommunication Science, College Park, MD
Enlighten IT, Linthicum Heights, MD
In-Q-Tel, Arlington, VA
Raytheon, Sterling, VA
International Business Machines (IBM), Washington DC
Hewlett Packard, Palo Alto, CA
Oracle, Redwood City, CA
Cisco, San Jose, CA
NVIDIA, Santa Clara, CA
Google Cloud, Mountain View, CA
National Air and Space Administration, Ames Research Center, Moffett Field, CA
SVB Capital, Menlo Park, CA
Defense Information Security Agency (DISA), Ft. Meade, MD

Field Studies – International

U.S. Embassy London, United Kingdom (UK)
One Trust, London, UK
Ministry of Defence, London, UK
Darktrace, London, UK
Cyber Defence School, Shrivenham, UK
U.S. Embassy Tallinn, Estonia
KeyStroke DNA, Tallinn, Estonia
Jobbatical, Tallinn, Estonia
Information System Authority, Tallinn, Estonia
Central Criminal Police, Tallinn, Estonia
NATO Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia
E-Estonia, Tallinn, Estonia
Wiseguys Startup Accelerator, Tallinn, Estonia
U.S. Embassy Brussels, Belgium
U.S. Mission to NATO, Brussels, Belgium
U.S. Mission to the European Union (EU), Brussels, Belgium
IBM Belgium, Brussels, Belgium
NATO Headquarters, Brussels, Belgium
Northrop Grumman UK, London, UK
National Cyber Security Centre, London, UK

Introduction

While the term 'cyber' is a shortened form of 'cyberspace,' cyber is often used as an adjective, verb, or noun. Cyber is most commonly understood as the complex combination of infrastructure, hardware, software, platforms, and general IT.

The U.S. is currently in a great power competition increasingly fueled by the information revolution within the ever-evolving cyber domain. Advanced computing transforms the global economy, e-business and every warfighting domain.[1] The U.S.' analysis, engagement and leadership in this revolutionary transformation is paramount to securing the future for our nation and for our allies.

To prepare future U.S. leaders and policy-makers and our international partners to prevail in this domain, the members of the Eisenhower School's Cyber Domain / Advanced Computing Industry Study (IS) examined a range of cyber and advanced computing technologies and explored the current state of the market of many key information technologies such as AI, blockchain, commercial cloud, and quantum computing. Additionally, the IS examined the challenges that the United States faces with respect to cybercrime, data privacy, protecting intellectual property (IP), supply chain vulnerabilities, accelerating the delivery of warfighting capabilities through modern software development practices, and a changing workforce.

The methodology used during the semester-long IS employed a variety of pedagogical approaches geared to a variety of learning styles, including: reading current topic-specific articles and literature, examining relevant market structures, student-led learning via case studies and knowledge-sharing, and discussions with experts from components of the triple helix (i.e., U.S. and foreign governments, industry and academia), and the iron triangle (i.e., Congress, Industry and Executive Branch). [2] Additionally, the IS met with private and government-backed venture capital firms to understand their approaches to investing in start-up companies, whether to help incubate or accelerate their ideas to the commercial market. The members of the IS also visited U.S. and foreign government organizations, such as the NATO Military Committee Working Group for Communication and Information Systems, the Estonian Information System Authority, U.S. Department of Homeland Security, U.S. Cyber Command, and the Defense Information Security Agency (DISA), to gain an appreciation and sense of the U.S., allies, and partner's cyberspace operations and capabilities to secure and defend the cyber domain.

Industry Definition

The cyber domain and advanced computing industries are wide-ranging and evolving sectors that encompass many different subjects. As there is no single "cyber industry," for ease of discussion in this paper, we will use the term "cyber industry" to represent the main industries among the computer-driven and interconnected technologies. Commonly, the term cyber evokes a variety of definitions especially as it becomes more intertwined in the many different facets of daily life. At a macro level, cyber and advanced computing includes information technology services, hardware, and software that function in the cyberspace domain.[3] Further dividing cyber and advanced computing industry into subsectors yields: products, services, computers, wireless, fixed line telecoms, software, application development, human capital management, training,

cyber insurance, semiconductors, processors, and internet services.[4] Key industry topics consist of the following primary and enabling technologies such as: 5G, internet of things (IoT), edge computing, AI, blockchain, cloud storage and computing services, quantum computing, autonomous vehicles, and cryptocurrencies.[5] With the delivery of these technologies, it will empower people to use resources beyond today's imagination which elevates the need to measure and understand the market.

To gain an appreciation for the vast size of the cyber and advanced computing industries, one need only view the multiple industry codes according to both the North American Industry Classification System (NAICS) and the Standard Industrial Classification (SIC). Most firms fall into multiple NAICS and SICs due to the diversification of the market (See Appendix A for a subset of the NAICS codes that make up the cyber industry). Some examples include Electronic Stores, Data Processing, Software Publishers, Custom Computer Programming, and Computer Systems Design. Some examples of leading, publicly-traded U.S. information technology firms are Apple, Microsoft, Google/Alphabet, Intel, IBM, Facebook, and Oracle.[6] All of these firms are in the Forbes Top 10 for global technology and are examples of the plurality of the market in which most firms generally provide both products and services along with hardware and software.

Current Condition of the Industry

As previously noted, there is no single "cyber industry." For that reason, this section examines the current conditions of the main distinct industries among the computer-driven and interconnected technologies essential to the cyber domain, including IT and telecommunications.

Current Competitive Structure

Industry competitive structure varies widely in the cyber domain. For example, despite the presence of a number of large multi-national companies with high name recognition in the IT consulting sector, market concentration is low and competition is high due to the rapid pace of technological change and low barriers to entry. While the larger, more well-known cloud and enterprise solution providers typically target large corporate clients, there are "thousands of smaller firms specializing in a specific technological platform, skillset or geographic area."[7] In contrast, the U.S. wireless telecommunications industry is highly concentrated, with four large companies (Verizon, AT&T, T-Mobile and Sprint) controlling the vast majority of industry revenues, and high competition among the firms within the sector because the industry's products and services are homogeneous. As of this writing, the U.S. Department of Justice is still considering whether a proposed merger between T-Mobile and Sprint would adversely impact competition. Wireless telecommunication companies also face increasing competition from rivals outside of the industry, such as cable companies.[8]

Firm Health

Simply by virtue of its size and breadth, the U.S. IT consulting industry is generally resilient. During the five-year period up to 2018, the industry's estimated annualized growth rate was 2.7% and average profit margins were estimated at 7.1% of industry revenue before interest and taxes.[9] As is typical of high knowledge-based service industries, wages represent the largest cost incurred by firms in the industry. Due to continued strong demand for IT services, it is estimated that wages accounted for approximately 48.4% of annual industry revenue in 2018,

which is up from 43.5% in 2013.[10] This stands in stark contrast to the wireless telecommunications industry where wages make up just 6.4% of revenue.[11] Driven by year over year increases in the number of mobile internet connections, the wireless telecommunications industry has performed well over the past five years. Revenue is projected to grow at an annualized rate of 1.1% to $289.4 billion through 2019, with revenue projected to increase by 3.4% in 2019 alone.[12]

Role of Firms' Business Units

Business units are important to large capitalization tech firms; for example, Facebook, Amazon and Google have steadily acquired smaller firms and start-ups to quickly access new technologies instead of developing those capabilities themselves. [13] In 2018, Facebook acquired PillPack in order to gain a foothold in the healthcare space, and also acquired the connected doorbell company Ring "to further its ambition to become the master of the smart home."[14]

Effective Business Strategies

Over the last decade, the dominant business strategy in the wireless telecommunications industry has been consolidation. The industry is extremely capital-intensive because of the need to invest in wireless telecommunications networks and infrastructure and obtain licenses for radio spectrum. Wireless telecommunications operators have consolidated in order to eliminate redundant costs, expand coverage and improve their profitability. In less capital-intensive industries such as software development or IT consulting, companies tend to focus on niche areas of expertise. In the cybersecurity industry for example, there are many different security technologies covering data centers, endpoints, mobile, remote and cloud operations, to name a few. Customers tend to buy security tools from more than one vendor.

Threats from Substitutes, Suppliers, Customers, or Foreign Competition

The primary threats to companies in the cyber domain are consolidation, mergers and acquisitions, IP theft, and the rapid pace of development of the overall industry. On the foreign front, U.S. innovation in software and hardware development has been targeted extensively by Chinese competitors and State-Owned Enterprises (SOEs). In telecommunications, the threat from suppliers and China are one and the same. China produces most of the hardware for the industry. The U.S. has divested itself from manufacturing responsibilities and, as an industry, has become "neuro-facturers," meaning producers of intellectual services rather than physical goods." [15] This de-facto "divestification" was also a key finding in response to Executive Order 13806 *Defense Industrial Base and Supply Chain Resiliency*, in the impacts of "Decoupling of Design and Manufacturing." [16]

The Nature of Foreign Competition

The bulk of the competition to the United States' cyber industry comes from China, Russia, the UK, and Israel. Israel and the UK are growing their representation in these industries and are a notable challenger but their market presence remain relatively small. Russia has a robust capability to develop effective cybersecurity applications with Russian developers among the most capable in the industry. However, from an industry standpoint, Russian corporations have lacked sufficient influence and access to pose a significant threat to the U.S. cyber marketplace.

Threats from China are the most urgent, particularly regarding IT hardware, software, and telecommunications. Over the last decade, the Chinese government has championed their industry's productivity extensively and will continue through 2025. Chinese leaders developed two primary initiatives to pursue this strategy, *Made in China 2025* and the *2006 Medium to Long Range Plan for Science and Technology*. [17] *Made in China 2025* is "an industrial upgrading strategy that aims to shift China's economy into higher value-added manufacturing sectors" such as robotics, aerospace, and emerging technologies, which include cybersecurity. [18] The 2006 plan focuses on leveraging government subsidies, heavy investments in research and innovation, and targets for local manufacturing content to build out emerging technology and industrial manufacturing advantages.

From an export standpoint, the U.S. has seen a great deal of its cyber domain IP compromised by China and Chinese companies. Much of China's industrial growth over the last two decades can be attributed to the commercialization of U.S. emerging technology IP. Economists believe that the theft of U.S. IP may have cut China's Research and Development (R&D) costs by two-thirds over the same period.[19] Due to these circumstances, experts believe that China may be able to technologically "leapfrog" and thereby overcome the U.S.'s dominant industry position and because of this, China is poised to pass the U.S. in several emerging technology and cyber-adjacent industries.[20]

Opportunities in Foreign Producer and Consumer Markets

The global cyber industry is robust with state governments and marketplaces increasing spending on cyber. Europe and the Middle East are growing markets for U.S. cyber exports and will continue to be so over the next five years. But, the primary opportunities for the U.S.'s cyber industry lie within Asia, and China specifically. However, several obstacles exist that complicate the U.S.'s ability to pursue those markets. Currently, the U.S. is imposing higher tariffs on Chinese goods and is seeking to negotiate trade deals with China that are more favorable to U.S. industry. The result is that many cybersecurity-related exports and imports are being captured by extensive tariff structures. Some experts believe these tariffs to be economically inefficient to U.S. businesses. The U.S. has executed tariffs on approximately $150 billion of Chinese goods.[21]

From a market standpoint, China's domestic industrial policy is based primarily on a significant investment and subsidy model. In China, local governments facilitate the buildout of these industries by contributing financial promissory notes, funding, and/or investment to enhance productivity and reduce labor costs.[22] China also offers some of these incentives to international businesses, including U.S. cyber firms, however with some significant qualifiers, such as the mandate for IP technology transfers. The IP threat remains one of the most serious challenges to the U.S.'s effective utility or access to Chinese and Asian markets.[23]

Challenges

Security

We live in a cyber-influenced world where an increasing number of devices are virtually connected. While this connectivity adds value to our economy and conveniences to the public, it also leaves us vulnerable to cyber criminals, espionage, and cyber warfare. Cybercrime affects our financial institutions, personnel databases, and other critical infrastructures that form the basis of our way of life. Malicious activity is now a constant persistent threat to individuals and societies as a whole. Attribution of cyberspace attacks is difficult and spans far beyond the stereotypical 'hackers' operating in their parents' basements. There are reports of coordinated activities by nation states, including Russia, that have breached critical systems (including electrical grids), denial of services to critical industries, exposure of millions of people's personal data, and attempts to sway the outcome of high-profile elections.[24]

Protecting cyber networks in today's digital world is required if we are to survive as a free and open society. Some efforts are being made in this effort, such as the EU's adoption of the General Data Protection Regulation (GDPR) that penalizes companies that negligently allow breaches of personal data. In the U.S., the National Institute of Standards and Technology created a voluntary framework for companies and operators of critical infrastructure to assess and improve upon their ability to prevent, detect, and respond to cyber attacks. However, as technology tends to advance more quickly than public policy, governments and other allied organizations are playing catch-up as they seek proper standards that balance security with liberty and innovation. Finally, as we begin to operate more and more 'in the cloud' and advances in AI, machine learning, and quantum computing continue to evolve, security must be a primary consideration and not an afterthought.

Supply Chain Security

Ensuring the security of equipment associated with cyber supply chains are becoming exponentially difficult with the continually increasing complexity, specialization, and globalization of product development and manufacturing of both software and hardware. Software companies are developing products by combining hundreds of smaller open-source code segments that execute very specific tasks into larger more complex products. These code segments are made by various vendors throughout the world and comprise of millions of lines of code that are difficult to thoroughly inspect for vulnerabilities. Hardware such as cell phones and networking equipment are often made and/or assembled in China using components that were manufactured in numerous countries. Validating these products and components are free of vulnerabilities, made to required specifications, and not tampered with prior to final assembly requires in-depth analysis and certification processes to be in place to ensure the industry remains secure.

Privacy and Data Security

A common theme one hears in the cyber industry is that that whomever owns the most data will be crowned king[25]. However, as humans readily connect to the IoT and freely navigate cyberspace at home and at work, this awareness of data collection is often subjugated to the pursuit of convenience. Privacy is naturally lost as we openly surrender our information and blindly sign digital terms of agreement without ever reading these increasingly lengthy legal documents. We must now come to terms with the fact that we are continuously surveyed and monitored even in

the sanctity of our own homes often without our direct knowledge.[26] People's thirst for social media engagement allows every aspect of one's life to be viewed, tracked, and stored for future use. Our conversations, downloads, searches, and everything else we do within reach of a connected device is susceptible to use by others, be it targeted advertisements or other, more nefarious intent. This collection of big data is consuming the industry as programmers build more and more sophisticated algorithms that feed the development of programs utilizing AI and machine learning. And although most intent is for the greater good and advancement of society, it is naive to think that malicious actors are not finding ways to weaponize this vast amount of structured data.

Intellectual Property Theft

Our adversaries are exploiting vulnerabilities in the cyber domain to steal intellectual property in an effort to gain a technological and economic advantage as a strategy in great power competition. It is estimated that intellectual property theft resulted in over $600 million in losses in 2017.[27] Adversaries, such as China, are exploiting vulnerabilities that exist as a result of increasing interdependencies and interconnectedness of networks across the public and private sector. They are targeting all aspects of the defense industrial base in an effort to maintain parity with the development of advanced weapon, communication, and intelligence systems. This is allowing adversaries to drastically lower investment costs and shorten research and development timelines, as well as overcome any disparity with maturity of defense industry partner capabilities.

Democratic Institutions

Given adversarial intent across the digital domain, only now are we starting to understand the vulnerabilities confronting democratic societies. Actions and policies must be employed to directly counter this threat; yet, these measures must be held in check to prevent free democracies from sacrificing liberties and inalienable rights commonly shared by every American. Unfortunately, state-controlled countries have a structured advantage over democratic societies to control social media output, promote industry direction in their favor, and execute state directed cyber offensive operations with greater ease. During our industry travel, the UK announced that it would incorporate non-core 5G components manufactured by Huawei into their telecommunications infrastructure even though the U.S., Australia, and other democratic nations have indicated a strict ban on the use of these Chinese products due to national security concerns.[28] With China and other nations generating less expensive IT hardware, forcing the hand of allied governments to follow the U.S.'s lead is extremely challenging with only limited financial resourcing. Other challenges stem from the human dimension of cyberspace. Studies indicate that younger Americans are now using social media as their primary source for news, which makes it difficult to combat disinformation described as 'fake news.'[29] The US must navigate through a complex balance of maintaining our democratic way of life while reducing democracies' vulnerabilities.

Human Capital

The exponential growth of the cyber domain has created a large demand for cyber professionals with skills in software programing, data science analytics, and cyber security. Every organization that the IS members visited, whether public or private, described recruiting and retaining skilled cyber professionals as one of their top challenges. The same was true for the foreign organizations visited in London, Brussels, and Estonia. In 2018-2019, cybersecurity skills

topped the list of greatest talent shortages in the United States with 53 percent of organizations surveyed reporting a problematic shortage of cybersecurity skills within their organization.[30] This global demand for talent has led to a drastic increase in compensation for personnel with cyber skills, and inadvertently created a serious challenge for the industry as government organizations struggle to compete with the private sector that has the ability to offer significantly higher wages.

Outlook

As the world becomes more digitally connected, our reliance on the efficiencies gained through advances in computing and associated technologies will continue to create vulnerabilities that malicious actors can exploit to threaten our security and prosperity. Despite these vulnerabilities, cybersecurity professionals generally agree that cutting-edge technologies like AI, IoT, quantum computing and blockchain will soon become the prevailing tools of our daily lives. There is little doubt that every sector of our economy will benefit greatly from advances in AI. In fact, there are examples in which AI solutions are already improving education, healthcare, cybersecurity and the finance. These solutions, along with the support of IoT devices and quantum computing, will further enhance the industry's ability to provide value and a competitive advantage to firms and organizations that leverage its benefits to generate substantial economic growth.

Public policy related to AI is needed, but it should be flexible enough to manage the full spectrum of AI use to ensure public trust, as governments and citizens try to balance the need for future advances with the risks of increasing malicious activity and irresponsible use of AI, such as AI-generated articles and videos (called "deep fakes").[31]. The exponential growth in digital data, coupled with advances in edge computing, is the lifeblood of this industry's future. Therefore, the great challenges of this century entail passing sound legislation and guidance that provides security and privacy of data, while ensuring that it remains accessible for commerce, defense and public security, healthcare, and, education.

It is estimated that there are already 26.7 billion devices connected to the internet and the number of connected devices will reach 75.4 billion in 2025 with an increase of 182.9 percent.[32] McKinsey Group estimates that "the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value would be equivalent to about 11% of the world's economy."[33] While possible economic gains from IoT are high, its largest obstacle to adoption is privacy and security concerns.[34] The connected devices are already a part of everyday life, and IoT is expanding without any security and privacy strategy.

According to a study conducted worldwide by Gartner in 2017, IoT security spending is expected to reach $1.5 billion in 2018, and, by 2022, half of all the security budgets for IoT will go to fault remediation, recalls and safety failures rather than protection.[35] To address the security and privacy issues of IoT, governments need to establish governing and advisory bodies, and with the help of these bodies, provide policies and standards, as well as incentives to compel the industry to follow the established measures.

The industry will maintain its preeminent force with the ability to support national security resources in the global marketplace. Not only because of the proliferation of IoT, AI and quantum computing, but also because it is buttressed against the insatiable need for data and the growing

demand for data analysis, data science and data security. In each of these areas of effort is an outcrop of markets and solutions that will support national security priorities. For instance, data security might involve the need for cloud and platform as a service as a means to protect core data. Additionally, it might call for data encryption services or data management solutions. With governments and firms facing increased attempts at data breaches and network exploitation, data security has become both an offensive and defensive effort and will continue to dominate the digital ecosystem for years to come.

Current impediments for the industry to achieve full surge and mobilization potential include a lack of information technology professionals in critical areas to include science, technology, engineering and mathematics (STEM) and data scientists. Based on these shortfalls there needs to be government incentives to entice people to pursue these areas of study such as: education grants at the undergraduate and post graduate level to enter these disciplines, military service incentives to change into an IT critical job, and incentives for civilians to do on-the-job training to enhance their IT skills.

The short-term outlook for the industry is a principal concern for the government and based on current conditions it will remain an imperative for the government for the next five years.[36] The government needs to allocate more resources to help mitigate the plethora of cyber attacks, reduce vulnerabilities and address debilitated critical infrastructure. As for the long-term outlook, the U.S. Federal cybersecurity market will reach an estimated $46 billion by 2030, with infrastructure hardening taking up a significant portion of the market. The industry will continue to develop improvements in cybersecurity methods and technologies as the United States' adversaries continue to exploit weakness across cyberspace.

Government Goals and Roles

U.S. cyber leadership is imperative to protect U.S. citizens and residents, corporations, and allies. The economic and global stability of the future are inextricably connected to a safe and secure digital infrastructure.

Cybersecurity represents both a threat and an opportunity for the long-term national and economic security of the United States. To ensure cyber trends lead to opportunity, the U.S. needs to leverage one of its key strengths, an innovation ecosystem founded on the triple helix, comprised of government, academia, and industry. The U.S. must find a balance between enacting prescriptive policies that could stifle innovation and those that protect U.S. citizens and firms, and uphold the rule of law. Recent Executive Orders to promote a cybersecurity workforce and voluntary programs to encourage critical infrastructure protection are two such examples. These unfunded mandates lack federal funding to regulate or incentivize industry and universities to align with government objectives. Congressional action and funding to further incentivize industry participation is the logical next step to promote actual cyber programs aligned to government policies. Cyber funding would dramatically increase the power of the triple helix to promote U.S. and international cybersecurity.

Today, U.S. cyber policy is a montage of state, federal, and international laws; these laws lack a federal homogenized framework to provide clarity on the US' cybersecurity position. One

of the largest cases under federal statute consideration is the Federal Trade Commission's (FTC) reinvestigation of Facebook. Facebook was implicated in the 2016 presidential election scandal for releasing personal data via third-party apps on the social media site violating the August 2012 Decision and Order from the Federal Trade Commission. The Decision and Order was the product of a suit filed through the Consumer Protection Division of the FTC against Facebook.[37] Interestingly, there is no federal statute that requires clear, continuous, and unambiguous notification of personal information releases. Six state and federal statutes are being used in the 13 current Facebook lawsuits regarding cyber-protection violations.[38] These acts are not clear on consumer information protection, storage, or information release notification. The California Consumer Protection Act is currently under a stay of execution awaiting a rewrite to ensure it comports with the European Union GDPR affording release and protection rights to consumers. Simplifying these often-conflicting statutes into a privacy protection framework would help protect consumers and firms while maintaining U.S. market agility.

The U.S. should glean ideas and best practices in policy, technology, and procedures from other countries that are pioneers in these areas, like Estonia. Today Estonia ranks third in the national cyber security index (NCSI).[39] The NCSI is a best practice developed by the Estonia Development Corporation, "measuring the preparedness of countries to prevent cyber threats and manage cyber incidents."[40] The framework considers nation state's legal posture, technical solutions, organizational support, capacity building, and civic cooperation as prerequisites for national cyber readiness.[41] In 2018, the U.S. placed 22nd on the list of one hundred nations assessed against the NSCI (Estonia is in second place). Estonia's National Cyber Security Strategy focuses on private-public partnerships, national cyber-hygiene education (kindergarten through college), developing strong information and communication technology configuration management, and employing 24/7 cyber protection teams are replicable practices.[42] The three pronged approach of public education, infrastructure management, and cyber response is central to Estonia's digital success and should inform U.S. national cyber policy development.

The U.S. should fill the White House 'Cyber Czar' post and continue promoting the NIST cybersecurity framework defining performance requirements, thereby allowing corporations to find the prescriptive means and methods to accomplish regulation. Compliance with the NIST cybersecurity framework is required for all cabinet agencies per Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.[43] Nevertheless, the USG has been slow to legislate or regulate the public sector - where most Personally Identifiable Information (PII) and personal preference data is stored, archived, and levied for business. National policy should address this trend.

New acquisition authorities and policies, such as Middle Tier Acquisition in the DoD, are paving the way for acquisition professionals, requirement owners, and industry to leverage more streamlined capabilities in a timely manner. Leadership should continue fostering rapid-agile acquisition practices for cyber services, development, and products - holding people accountable for their mistakes while not stifling innovation and reasonable risk taking.

Developing human capital in cyber is imperative to the U.S.' success. One way to develop this skill set would be to stand up a 'Cyber Reserve Corps.' Developing this federal acumen should be priority number one. The lack of sufficient skilled/experienced personnel for cyber operations

are vulnerabilities in the U.S,' war fighting capabilities. While the U.S. is making a significant investment in cyber defensive measures such as training and educating critical infrastructure industries, raising cybersecurity awareness, and establishing youth development programs, more is required. The reservist program would offer intense training, require participant pay-back in years of federal service, and offer prorated tuition forgiveness. Federal cyber warriors would be a part-time reserve unit building a "bench" of cyber action teams. Cyber corps enlistees during normal business hours would infuse IT trained soldiers into the civilian market creating a win-win for employers, the U.S., and U.S. IT employers.

Because the cyber domain is international and ubiquitous, it is insufficient for the U.S. to formulate a U.S.-only cyber policy to deal with the aforementioned issues. As a nation that leads the free world, the U.S. must do so at the international level as it does in many other areas. The U.S. should help shape the creation of international norms in the cyberspace domain through partnerships and alliances. To do this, the U.S. should strengthen international organizations, such as NATO and the United Nations, and use economic and political tools such as incentives and sanctions to support policy and regulation implementation.

The current President of the United States stated that the, "cyber threat is one of the most serious economic and national security challenges we face as a nation."[44] The threat is real, the damage is significant, and the impacts are far reaching. A coherent, agile, and internationally coordinated cyber policy must be devised to provide security and to ensure that citizens can safely participate in the information/digital revolution.

Essays on Major Cyber Issues

Industry Study seminar members provided the following brief research essays, which cover three general areas: Cyber Acquisition, International Cyber Partnerships, and Securing the Cyber Domain. Appendix B contains a full list of individual research papers.

Cyber Acquisition

Normalizing Acquisition of Offensive Cyberspace Operations Weapon Systems

Cyberspace is the newest of the warfighting domains and has its own organizational structure and unique authorities granted to conduct offensive cyberspace operations (OCO); we therefore need to develop a relevant acquisition strategy. A challenge that developers of offensive cyberspace capabilities face is the overwhelming number of alliances looking for and sharing vulnerabilities to commercial products in order to secure them and make them less vulnerable. Offensive capabilities either exploit zero-day vulnerabilities or other means to gain access to adversary networks, so it involves constant research to find and develop exploits. The preferred development methodologies are agile for software development and DevSecOps (Development-Security-Operations) for development in general.

The recommendation for Offensive Cyberspace Operations is to develop an acquisition strategy that leverages a modular open system architecture core platform for many joint functions such as command and control, maneuver, information and assessment, as well as interface control documents for developers to produce the cyber effects. The core platform would follow a more traditional development approach outlined in DoD Instruction 5000.02, and the effects could be developed under Middle Tier Acquisition authorities to get prototypes fielded more quickly.

Mr. Ric K. Nordgren

Facing the Challenge of Cyber Capability Acquisition for U.S. National Security

This essay discusses the challenge of cyber capability acquisition for U.S. national security through an analysis of the perspectives of key stakeholders facing this challenge. The stakeholders form an iron triangle consisting of the Department of Defense (DoD), industry partners who provide cyber and information technology (IT) capabilities, and our Legislative and Executive Branches. A fourth stakeholder, DoD's acquisition community, lies in the middle of this iron triangle and is subjected to the influences of the three triangle corners. As cyber capabilities consist mainly of IT hardware, software, and services, it follows that the four stakeholders should, but collectively do not, possess the required level of cyber and IT awareness, expertise, or experience to effectively face the cyber capability acquisition challenge. Therefore, a paradigmatic shift is needed to comport to this challenge.

The stakeholders collectively need to escape the burden of bureaucratic thinking and routine legislative guidance regarding cyber and IT acquisition. After decades of malicious cyber incidents, stolen information and intellectual property, and privacy compromises, it is dawning on many, but not yet all, that IT as cyber is a national security matter. The following recommendations change the existing paradigm: Congress and the President should create the term 'National Information System' (NIS) to cover all IT used by the federal government or by any public or private entity conducting business with the federal government; create a cyber 'color' (i.e. category) of funding that can function inside the annual DoD budget cycle; and, permit some amount of cyber capability acquisition in the field that is outside routine acquisition systems. DoD's acquisition community can evolve to effectively address the cyber challenge, but only if the stakeholders at the corners of the iron triangle cohesively evolve first. Only then can we face the challenge of cyber capability acquisition for U.S. national security.

Mr. Michael R. Cirillo

Cyber Capability Development Using the Agile and DevSecOps Methods

The Department of Defense (DoD) should consider incorporating new private sector approaches into the cyber tool acquisition process. These new tools could include the Agile and Development-Security-Operations ("DevSecOps") methods. The cyberspace domain is often misunderstood for what it is and what it is not. This lack of understanding is further intensified in both cyber capability development and acquisition processes in a constantly evolving cyber domain. Not only do the tools advance rapidly, but the environment and the threat actors they are used against change, too. Given that nation states, criminal hackers, and Violent Extremist Organizations are constantly conducting offensive operations against the United States, we need a flexible acquisition system that allows for rapid purchase and updates of tools to fulfill the offensive mission set. Rules and methods designed to squeeze out risk should not hinder the acquisition of cyber tools. It is also crucial to recognize the role of culture as well as organizational frameworks, as new or modified processes will not necessarily fix the situation if the culture and values of the acquisition community do not adapt to change.

DoD needs to incorporate new industry approaches such as Agile and DevSecOps into the cyber tool acquisition paradigm. Those methods include open discussion between the user, developer, and staffs. Adhering to Agile and DevSecOps methods places the developer and user together during the test-field-deploy process, which allows for rapid changes and patching updates during offensive operations. Due to the effects on market structure, noncompetitive contracting should be judiciously used, as a cleared tool developer market is highly susceptible to consolidation and exit due to its size. The pooling of qualified, cleared contractors similar to other prime vendor programs and broad area announcements can prevent a market concentration that is unfavorable to future procurements and would also diversify the tools. It is important for organizations that want to incorporate Agile and DevSecOps in their tool development processes to assess and build (or change if necessary) their organizational culture and acquisition framework. Doing so will facilitate the implementation of innovative concepts, thereby meeting the demands of cyber operators.

LtCol Paul Gillikin

International Cyber Partnerships

Sharing U.S.-Based Cybersecurity Frameworks with NATO

There are various American cybersecurity frameworks that the North Atlantic Treaty Organization (NATO) could consider for adoption in order to strengthen their common defense. Even while responsible for collective defense and cooperative security within a diverse membership, NATO recognizes that global security has increasingly become dependent on data. Organizations now must communicate their cybersecurity posture in a data-rich way that identifies, assesses and mitigates the potential risk to their information systems. The anonymity and complexity of cyber attacks has ushered in an era of hybrid warfare that challenges the ability of western democracies to work together. A comprehensive cybersecurity framework addresses these challenges and raises the awareness of the risks of today's sophisticated, rapidly-spreading cyber threats. Further, it enables organizations to identify standards and guidelines to protect critical systems and share best practices that enhance their security efforts.

We examined three industry-leading cyber frameworks: Office of the Director of National Intelligence / Department of Defense Cybersecurity analysis and Review, Cyber Resiliency Review, and the Business Software Alliance. Each of these has unique capabilities as well as commonalities. Through our analysis, we determined there is not a one-size-fits-all approach to defend against cyber attacks. Instead, we advocated an approach similar to the one deployed by former NATO Supreme Allied Commander Europe, Admiral James Stavridis. He supported "open source" security in which nations, the public and private sectors work in partnership to achieve collective security. We asserted that leveraging specific areas of each would complement the existing NATO efforts. With limited resources, prioritizing the alliance's main efforts and being nimble enough to implement industry best practices might be ideal for NATO.

Colonel Patrick Curry, Lieutenant Colonel Edward Kendal, Commander Derrick Blackston and Mr. David Vargas

Strengthening Cyber Alliances and Partnerships

There is an urgent need to formulate U.S. Government policies to leverage U.S. cyber capabilities to strengthen alliances and attract new partnerships. The world is facing the 'rise of the machines' era, which is digitally connected, dependent yet vulnerable, and where all things are hackable. The possible detrimental impacts from cyber threats can impact individuals as well as nations, including cyber-nuclear threats, from known and unknown sources, leading to the unquestionably urgent needs for cybersecurity and protection. In order to materialize the national and global security objectives, these require strategic policies that can facilitate highly coordinated efforts, not only among the U.S. Government, industries and academic institutions, but also, among allied governments. These policies must be comprehensive so as to cover dimensions such as politics, economic, social, technological, legal, environmental, and military.

U.S. efforts are needed to shape the common preferred environments to be well-equipped with cyber capabilities and to strengthen alliances and attract new partnerships. A cyber-capable

coalition can ensure that the United States and its allies can successfully counter any potential regional hegemons. The U.S. wartime readiness and preparedness includes the capability to mobilize its resources to support various combatant commands in a timely manner. Having common platforms for cyber capabilities and also, policies will further facilitate interoperability for joint and combined exercises and operations. The policy formulation requires strong political will from the U.S. Government and the nations and the global communities concerted efforts, to materialize all levels of security objectives. Cyber threats are real and could be detrimental to individuals, business entities, countries and multilateral organizations. As policy is the most effective means to deter the negative impacts of cyber threats, we have no choice but to implement it to the highest degree.

Brigadier General Shamsudin Kassim

The Case for a U.S.-Middle East "Friendship Cyber Pact"

In order to counter Iran's malign influence in cyberspace across the Middle East (ME) and beyond, the United States should spearhead a strong and cohesive economic and technological partnership among ME nations, including Israel, focused on cybersecurity. This initiative would entail establishing a "Friendship Cyber Pact" (FCP) to develop capacities in cyberspace and advanced computing as main partnership growth generators. The United States should work with the moderate Arab countries to help them strengthen their technology sectors in order to challenge Iran's technological superiority. Focusing on emerging technologies, cyberspace and innovation will give the pact's partners a long-term relative advantage. Israel's participation here is critical, as a result of its technology and innovation advancements.

Cooperation should be built gradually, starting with developing the future generation of computer engineers and programmers under the umbrella of the FCP, then focusing on strengthening the physical cyber infrastructure of FCP countries. The FCP should harness cyber and advanced computing to innovate in areas of broad consensus such as: water purification, renewable energy, and agricultural innovation. Next, the FCP can collaborate on cyber defense against Iranian cyber attacks. This strategy should be based on creating cyber technological advantages that will generate economic growth, develop necessary defense capabilities, improve education, and influence rule of law and common values. In this way, the U.S. and its FCP allies can confront Iran in the cyber realm, by employing what is known in Arabic as "Muqawamah" (a strong resistance). This joint effort will create the technological advantages needed to stabilize allies' economies and to stop Iranian influence and expansion, thereby ultimately, increasing the chances for peace in the Middle East.

Colonel Shlomo Binder

Promoting Cyber Policies Towards Gulf Cooperation Council Allies to Confront Iran

The Gulf Cooperation Council (GCC), comprised of six member nations, plays an important role in the Middle East's Arabian Gulf region in shaping the political, military, economic and socio-culture cooperation and coordination among its members. As this is a region of strategic importance to the United States and its allies, more attention needs to be given to the area's

cybersecurity. The GCC countries are surrounded by the Islamic Republic of Iran which is considered as a destabilizing force which threatens western powers' interests in the region, including the United States. In the past decade, the GCC countries have become increasingly modernized and digitalized their critical infrastructures and private industrial bases. However, the region's cybersecurity institutions are still new, leaving the financial and governmental bodies vulnerable to many external cyber attacks. These provide a greater opportunity for exploitation by hackers and other bad actors in cyberspace.

Cybersecurity is an increasingly important concern with growing dependence on the defense and non-defense networks and systems. The GCC region is in a period of transition to the digital world, including national and military defense technology. The GCC should invest resources to promote their cybersecurity in cybersecurity infrastructure, relevant laws, and regulations. Also, they should protect other western allies including U.S. interests and infrastructures on their soil. The GCC states, however, face many challenges in cyberwarfare internally and externally including from Iran's growing cyber capabilities and influence in the region. As this region is vital to the U.S. national security due to energy networks and location of military assets, the U.S. should first address this issue bilaterally and then multilaterally by promoting U.S.-GCC cyber capabilities via establishing several joint dialogs and training initiatives. By doing so, the GCC benefits from the U.S. experiences and its cyber industries. The U.S., in turn, benefits by protecting its infrastructure and its interests in the area from adversaries and reduces the frequent and potentially adverse impact of critical technology transfers to U.S. adversaries in the region.

Commander Ahmed Al Busaidi

Securing the Cyber Domain

Cyber Supply Chain Integrity

This essay discusses cyber supply chain integrity. Cyber supply chain is vitally important to national security and must be addressed with a sustainable solution. The DoD has a significant problem with counterfeit microelectronics that stems from the outsourcing of production to other nations. This is not necessarily nefarious in nature; it is a byproduct of globalization. U.S. suppliers who produced many of the microelectronics used in DoD platforms have ceased to exist, outsourced their demand because producing spare parts is no longer profitable, or have been acquired by or merged with other firms. In fact, more than 90 percent of obsolete parts in the DoD are microelectronics.

For the DoD to regain trust in its microelectronic suppliers, a combination of methods must be used. While currently deployed methods of sourcing trust and tamper-proof tracing help, a system of governance would add layers of transparency to the process. Blockchain is an ideal candidate to provide this system of governance that increases trust and transparency in the cyber supply chain. With its complete supply chain transparency from its origin to delivery method, blockchain offers tremendous potential for DoD users that struggle with counterfeit parts. While commercial adoption has been slow, a DoD regulated system would garner the trust of industry

partners and ultimately lead to the DoD's ability to achieve national security objectives by delivering the RIGHT part, all the time!

Lt Col Matthew Belle

Securing the Internet of Things

The number of Internet-connected devices continues to increase and do so almost exponentially. The diversity of these devices is beginning to include items never before thought of having a need to connect to the network; e.g., televisions, kitchen and healthcare appliances, and cars. With this rapidly growing number of devices connected to the internet, a new term has entered into our daily lexicon, known as the "Internet of Things" or IoT. IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. The connected devices are already a part of everyday life and IoT is expanding with limited security or with a cohesive privacy strategy. This creates risks up to and those affecting national security.

To address these risks, governments need to establish governing and advisory bodies to provide policies and standards regarding IoT, as well as incentives to compel the industry to follow the established measures. Industry must accept the security of IoT as a design parameter from the beginning rather than an additional layer incorporated into a system after production. Because IoT is an expanding new area that touches on all aspects of daily life, users become the critical link in providing security and privacy for IoT. Users need to be informed about threats, proper IoT operations and how to protect their information. Without proper knowledge of future systems and services, all the security and privacy concerns cannot be addressed thoroughly. Studies on these issues should be conducted in a holistic approach. Failing this, it will be the users who ultimately pay for the convenience and affordability of new technologies that come with IoT, thereby sacrificing their security and privacy; that is too high price to pay.

Colonel Suleyman Ugural

A National Security Imperative in Cyberspace: The Need to Mobilize Human Resources

There is an understated human resource dynamic underscoring the challenges of the cyber and advanced computing industry. The U.S. labor market is lagging in Science, Technology, Engineering and Mathematics (STEM) knowledge as well as in core trade skills which are needed to ensure the holistic health of the defense ecosystem. This lack of supply of people entails inherent risk, including a decline in production capacity and decreased innovation. At the same time, due to changing demographics, a rapidly globalizing economy, and trends in education, the demand for tech-savvy employees is growing faster in the U.S. than the supply.

A common theme throughout our Cyber Domain Study was the lack of experts in Data Science and Analytics, which is an emerging interdisciplinary field that uses algorithms to extract meaningful insights from various data sources. Compared to other domains, cyberspace is unique in that conflict occurs continuously below the level of armed conflict, as evidenced by cyber

attacks on critical infrastructure and U.S. elections. Rather than continue the past practice of mobilizing military forces during wartime and demobilizing during peacetime, the U.S. needs to develop highly-qualified personnel able to engage in the cyber fight on a continuous basis.

We conclude that the U.S. is at an inflection point as changes in technology outpace the sum of the IT workforce, trade skill gaps hinder industrial production, and the lack of STEM graduates fails to meet the demands of government and the defense industrial base. We are at risk of failing in the defense of our nation and our national security, even while other nations seek to surpass the U.S. in cyber capability and in cyberspace. The time to act is now!

Col Patrick Curry and Ms. Allison Lee

Cyber Insurance

The market for cyber insurance products is expanding and is evolving to meet the needs to the unique cybersecurity ecosystem. Cyber insurance, also called cyber liability insurance and cybersecurity insurance, refers to a range of insurance products that cover a wide range of risks arising from the use of electronic data and its transmission, tools such as the Internet and telecommunications networks, physical damage caused by cyber attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information. The economic arguments in favor of cyber insurance are that it leads companies to make greater investments in cybersecurity, that it leads to establishment of cybersecurity best practices, and that it increases societal welfare by providing a mechanism for risk transfer.

Although the cyber insurance market is currently a very small portion of the total insurance market, the amount of policies written continues to increase. U.S. cyber liability insurance is the most developed, but expectations are that the European market will grow because of the European Union's 2018 General Data Protection Regulation law. Underwriters of cyber insurance have struggled with how to assess, quantify and price cyber risk. Some insurers consider whether to extend cyber insurance coverage by relying on written questionnaires submitted by potential customers about their cybersecurity and incident response practices. Insurers may also begin using Artificial Intelligence and machine learning to price risk and evolve away from actuarial tables. Insurers themselves have helped fund the growth of the cyber insurance market and it appears this trend will continue.

Colonel Jacqueline Emanuel

Improving U.S. Critical Infrastructure Cybersecurity Before Catastrophe Strikes

Some of the most critical U.S. infrastructure systems are highly vulnerable to cyber attacks, threatening the nation's long-term national and economic security. Today, the energy network is already experiencing attacks and the Department of Homeland Security has publicly acknowledged this. These public attacks, which occurred on two separate energy critical infrastructure penetrations were publicly traced back to a Russian government-owned technical research institute in Moscow. Disruption or, even worse, destruction of this critical infrastructure

would have a devastating effect on our physical and economic security. The U.S. can reduce critical infrastructure cybersecurity vulnerabilities and impacts by developing and procuring modern cybersecurity tools to prevent, detect, and mitigate cyber vulnerabilities and attacks.

Currently, because of the limited power of executive orders, critical infrastructure cybersecurity assessments are voluntary programs. Legislation to mandate cybersecurity assessments of critical infrastructure and to provide public-private partner funding to mitigate key vulnerabilities would significantly advance U.S. critical infrastructure cybersecurity. Cybersecurity tools are available that help prevent, detect, and mitigate vulnerabilities and, with help from their governments, are currently being deployed in other countries. The U.S. needs a focused effort to test and deploy modern cybersecurity tools to our critical infrastructure industries before catastrophe strikes.

Lt Col Ty Miller

Social Media Influences on Democratic Institutions

Humans are social by nature and group themselves together within communities of like interests. Today's digital environment, and especially social media, enhances the ability for people to connect. The downside is that we are only now starting to understand the risks to democratic societies given adversarial intent across the digital domain. For example, the 2016 U.S. Presidential election was heavily targeted by Russia's disinformation campaigns and hacking of servers in order to sway voters. Russia is not the only country using this tactic, however, and several dozen countries are publicly known to have had conducted organized disinformation campaigns in 2018. The use of disinformation, sometimes called 'propaganda,' to influence public opinion is not new, but combining disinformation with social media is fairly new.

The Internet is an open source where Americans should be free to explore, communicate, conduct commerce, and interact freely with others. Authoritarian nations like China and Russia have an advantage in cyber efforts to undermine democratic governments in that they share a dominant control over their media outlets, militarize civilian online activities to foster government goals, and disregard ethics when operating on the Internet. Democratic governments are now realizing that social media influence from adversarial actors is a constant threat because the psychology of interpersonal interactions is the focus of effort. A strong cultural shift in Internet usage is required, which should promote cyber hygiene across democratic countries needs at the earliest age and almost on par with how we, as humans, learn to walk or speak. Only until we truly focus on a cultural shift in how we use the Internet to connect with others, military and governmental defensive measures against cyber threats will only go so far.

Colonel Edward Meyers and Ms. Allison Lee

The Need for a Strategic Cybersecurity Policy

Given that cyberspace is the new frontier, the new domain of dominance, and the transformational technology of the 21st century, the United States needs to devise a strategic cybersecurity policy. In cyberspace, cyber state borders are illusive and knowing who is being a

cyber attack, also known as ‘attribution.’ is difficult. Effective cybersecurity policy must be global in scope, application, and vision, hence include the following:

- A performance requirement for data protection, data storage and release notification.
- Statutory codification of the National Institute of Standards and Technology cybersecurity framework, which identifies levels and types of data protection.
- A hierarchy of protected infrastructure, data, and IT systems with special consideration given to continuity of operation sites, military assets, national critical infrastructure, and the supply chain.
- Maintenance and mapping of the chain of custody, configuration management systems, and network architectures.
- Cyber hygiene training that is mandatory for cyberspace stewardship.
- Cybersecurity policy must engender international cooperation and rule of law such that global inclusion in a digital transformation enables ideals to subordinate sectarianism.

Transformational, visionary leaders are critical to the success of policy. We need these leadership gifts, skills, and abilities now, in order for the greater good, for the sake of humanity, to affect the course of history. We must feel compelled to sacrifice in the present for the future. Choosing leaders with vision, who eschew fear, inspire goodness as the path to greatness, and embrace humanity will put the U.S. on the correct side of policy in the digital revolution.

Mr. Anthony Burke

Conclusion

The overall state of the cyber and advanced computing industry is economically healthy and robust but faces security challenges. While the U.S. is still the world leader, cyber is redefining global norms in commerce, communication, and warfighting, as well as creating new threats. The U.S.' engagement, innovation, and leadership in this industry is paramount to secure the future for our citizens, our nation, and our international partners.

The multi-faced cyber industry is experiencing high growth and high return margins, but the current major shift to cloud services and the development of secure, transformational technologies is outpacing established statutes, regulatory efficacy, and legislative capability. The digital explosion has left networks either unprotected or progressively more vulnerable. It has also created a poorly protected and unaware citizenry at risk of data theft, and that is susceptible to cybercrimes. The increase in ubiquitous wireless networks and connected devices exponentially accelerates connectivity, information sharing, and risks. These changes need balance within a national security framework that provides protections but ensures liberty and nurtures innovation. Advanced computing in AI, machine learning, and quantum computing accelerate this digital transformation, potentially further exacerbating existing risks.

From a nation-state perspective, China represents the greatest threat to U.S. national interests in cyber and advanced computing. China's cyber industry is well funded as a state-owned and state-controlled enterprise. China's population is greater than the U.S.'s population, hence China offers a larger undeveloped market, untapped human capital potential, and a geographical hub for emerging Indo-Pacific economies. China is also the greatest perpetrator of intellectual property theft from the United States. The U.S. free market approach and protections for individuals' rights are at odds with China's autocratic government. Aligning U.S. values with Chinese ambitions is a significant challenge requiring strategic redress along a strategic timeline.

Cyber threats and opportunities are pervasive through the entire national security apparatus. The U.S.G. works with industry and academia, i.e. the triple helix," to leverage academia's technology with business incubators to stimulate economic growth. U.S. investments should continue to focus on developing this synergy to address threats and create opportunities. The U.S. must establish smart and robust data protection laws to protect its citizens and enable development of cyber-savvy leadership that can nurture international cyber norms and foster global cooperation. Our industry study provided a good overview of national and international markets and governmental engagement. The national security and resourcing strategy challenge is to position ourselves to capitalize on our national potential and ensure this industry's global benefit for all.

Appendix A: Industry Codes Related to Cyber

Category	NAICS	Title	Industry Definition[1]	Firms[2]
IT Hardware	33421	U.S. Telecommunication Networking Equipment Manufacturing	Manufactures wired (voice and data) telecommunications equipment; e.g., telephone switching systems, telephones, answering machines, data bridges, routers, modems and gateways	Northrop Grumman, Lucent Technologies, Siemens Planning
	33422	U.S. Communication Equipment Manufacturing	Primarily manufactures broadcasting and other wireless communication equipment.	Sierra Nevada Corp, L3 Technologies Inc., Orbital ATK
	33411	U.S. Computer and Peripheral Equipment Manufacturing	Primarily engaged in manufacturing and/or assembling electronic computers; e.g., mainframes, personal computers, laptops, and servers; and computer peripheral equipment, such as storage devices, printers, monitors, and input/output devices and terminals.	Hewlett Packard Co., Unisys, PNY Technologies Inc., IBM Corp., Dell EMC, SanDisk, Acer America
	33441	U.S. Semiconductor and Other Electronic Manufacturing	Manufacturing semiconductors and other components for electronic applications	Intel Corp., Micron Technology Inc., Cree Inc., Microchip Technology Inc.
IT Services	54151	U.S. IT Consulting	Primarily engaged in providing expertise in the field of IT through one or more of the following: (1) writing, modifying, testing, and supporting software to meet the needs of a particular customer; (2) planning and designing computer systems that integrate computer hardware, software, and communication technologies; (3) on-site management and operation of clients' computer systems and/or data processing facilities; and (4) other professional and technical computer related advice and services.	Oracle Corp., Science Applications International Corp., CACI International Inc., Dropbox Inc., Telecordia Technologies Inc.
	518210	U.S. Data Processing and Hosting Services	Comprises establishments primarily engaged in providing infrastructure for hosting or data processing services. These establishments may provide specialized hosting activities, such as Web hosting, streaming services, or application hosting (except software publishing), or provide general time-share mainframe facilities to clients. Data processing establishments provide complete processing and specialized reports from data supplied by clients or provide automated data processing and data entry services.	Google Inc., Amazon.com Inc., Seagate Technology Inc., Intuit Inc., Facebook Inc., Rackspace US Inc., Yelp Inc.

[1] North American Industry Classification System, 2017 NAICS Definitions, accessed May 10, 2019, https://www.census.gov/cgi-bin/sssd/naics/naicsrch.
[2] SICCODE.com, accessed May 10, 2019, https://siccode.com/search-business/

Category	NAICS	Title	Industry Definition	Firms
IT Services (cont'd)	519130	Internet Publishing and Broadcasting and Web Search Portals in the U.S.	Comprises establishments primarily engaged in (1) publishing and/or broadcasting content on the Internet exclusively or (2) operating Web sites that use a search engine to generate and maintain extensive databases of Internet addresses and content in an easily searchable format (and known as Web search portals). The publishing and broadcasting establishments in this industry do not provide traditional (non-Internet) versions of the content that they publish or broadcast. They provide textual, audio, and/or video content of general or specific interest on the Internet exclusively. Establishments known as Web search portals often provide additional Internet services, such as email, connections to other Web sites, auctions, news, and other limited content, and serve as a home base for Internet users.	Google Inc
Software	511210	Software Publishers in the U.S.	Comprises establishments primarily engaged in computer software publishing or publishing and reproduction. Establishments in this industry carry out operations necessary for producing and distributing computer software, such as designing, providing documentation, assisting in installation, and providing support services to software purchasers. These establishments may design, develop, and publish, or publish only. These establishments may publish and distribute software remotely through subscriptions and downloads.	SAP America Inc., Apple Inc., Paychex Inc., Electronic Arts Inc., Unisys Corp., Quantum Corp.

Category	NAICS	Title	Industry Definition	Firms
Telecom Services	517312	Wireless Telecommunications Carriers in the U.S.	Comprises establishments primarily engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular phone services, paging services, wireless Internet access, and wireless video services.	Verizon, Life Alert, Cal Coast Telecom, Medflight, AT&T, Pay Go Wireless
	517311	Wired Telecommunications Carriers in the U.S.	Comprises establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired telecommunications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services; wired (cable) audio and video programming distribution; and wired broadband Internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.	Unicorn Group, Yorktel Telecom Corp., Lyman Bros Inc., American Internet Service, DigitalGlobe Inc., Bonneville Satellite Co, US Signal
	517911	Telecommunications Resellers in the U.S.	Comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry.	Verizon Communications Inc., CenturyLink Inc., Cincinnati Bell Inc., Vonage Holdings Corp., Comcast Corp.
	517410	Satellite Telecommunications in the U.S.	Comprises establishments primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications.	Iridium Satellite, Intelsat General Corp., The Boeing Corp., Raytheon Company, American Government Services

Appendix B: List of Topics of Individual Research Papers

Belle, Matt, "Cyber Supply Chain Integrity." Cyber Domain/Advanced Computing Industry Study paper, Eisenhower School (ES), National Defense University (NDU), 2019.

Binder, Shlomo, "Counter Cyber 'Muqawama'" (relates to The Case for a Friendship Cyber Pact in the Middle East). Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Blackston, Derrick, Curry, Pat, Kendall, Ed, and Vargas, David, "Sharing U.S.-Based Cybersecurity Frameworks with NATO." Presentation to the North Atlantic Treaty Organization, Military Committee Working Group for Communication and Information Systems, Brussels, Belgium, April 30, 2019.

Burke, Anthony, "The Need for a Strategic Cybersecurity Policy." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

al-Busaidi, Ahmed, "Promoting Cyber Policies Towards Gulf Cooperation Council (GCC) allies to Confront Iran." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Cirillo, Michael, "Facing the Challenges of Cyber Capability Acquisition for U.S. National Security." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Curry, Pat, "Labor Market Dynamics to Mobilize a Nation." Individual Strategic Research Paper, ES, NDU, 2019.

Emanuel, Jacquelin, "Cyber Insurance." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Gilliken, Paul, "Cyber Capability Development Using the Agile and DevSecOps Methods." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Kassim, Shamsudin, "Strengthening Cyber Alliances and Partnerships." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Lee, Allison, "A National Security Imperative in Cyberspace: The Need to Mobilize Human Resources." Individual Strategic Research Paper, ES, NDU, 2019.

Lee, Allison, "Something Old, Something New: How Disinformation in the Age of Social Media Undermines Democracy" Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Meyers, Ed, "A Clear and Present Danger: The Threat of Social Media Influences on Democratic Institutions." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Miller, Ty, "Improving U.S. Critical Infrastructure Cybersecurity Before Catastrophe Strikes." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Nordgren, Ric, "Normalizing Acquisition of Offensive Cyberspace Operations Weapon Systems." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Ugural, Suleyman, "Securing the Internet of Things." Cyber Domain/Advanced Computing Industry Study paper, ES, NDU, 2019.

Endnotes

1 Jim Mattis, "Summary of the National Defense Strategy of The United States of America," *Department of Defense*, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (Accessed 9 May 2019).
2. Henry Etzkowtiz, *The Triple Helix: University—Industry—Government Innovation and Entrepreneurship*, 2nd Ed. (New York: Routledge 2008), 113.
3. Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *NDU Press* 73 (April 1, 2014): 14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf?ver=2014-04-01-122156-563 (Accessed 8 May 2019).
4. Andrew Nichols, "The Cyber Domain/Advanced Computing Industry Study," (National Defense University, Washington D.C., 2019).
5. Ibid.
6. Kristen Stoller, "The World's Largest Tech Companies 2018: Apple, Samsung Take Top Spots Again," *Forbes*, June 6, 2018.
7. Marisa Lifschutz, "IT Consulting in the US: 54151," *IBISWorld.com*, December 2018, https://www.ibisworld.com/industry-trends/market-research-reports/professional-scientific-technical-services/professional-scientific-technical-services/it-consulting.html (Accessed 7 May 2019).
8. Evan Hoffman, "Wireless Telecommunications Carriers in the US: 51721," *IBISWorld.com*, December 2018, https://www.ibisworld.com/industry-trends/market-research-reports/information/broadcasting-telecommunications/wireless-telecommunications-carriers.html (Accessed 7 May 2019).
9. Marisa Lifschutz, "IT Consulting in the US: 54151," *IBISWorld.com*, December 2018, https://www.ibisworld.com/industry-trends/market-research-reports/professional-scientific-technical-services/professional-scientific-technical-services/it-consulting.html (Accessed 7 May, 2019).
10. Ibid.
11. Evan Hoffman, "Wireless Telecommunications Carriers in the US: 51721," *IBISWorld.com*, December 2018, https://www.ibisworld.com/industry-trends/market-research-reports/information/broadcasting-telecommunications/wireless-telecommunications-carriers.html (Accessed 7 May 2019).
12. Ibid.
13. Savannah Dowling, "What Facebook, Apple, Amazon, Google, And Netflix Have Acquired In 2018," *Crunchbase News.com*, November 12, 2018, https://news.crunchbase.com/news/what-facebook-apple-amazon-google-and-netflix-have-acquired-in-2018/ (Accessed 7 May 2019).
14. Ibid.
15. Satya Kandala. "What Happened to US Manufacturing?," *Tuck School of Business.edu*, 28 Feb 2019, https://www.tuck.dartmouth.edu/news/articles/tuck-professor-uses-microdata-to-study-manufacturing-employment-decline (Accessed 8 May 2019)
16. DOD Interagency Task Force, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, *Defense.gov*, September 2018, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/Assessing-And-Strengthening-The-Manufacturing-And%20defense-Industrial-Base-And-Supply-Chain-Resiliency.pdf (Accessed 9 Apr 2019).
17. Kristen Hopewell. "What is 'Made in China 2025' — and Why Is It A Threat to Trump's Trade Goals?," *Washington Post Online*, 3 May 2018, https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/03/what-is-made-in-china-2025-and-why-is-it-a-threat-to-trumps-trade-goals/?utm_term=.a222877901a3 (Accessed 14 April 2019)
18. Ibid.
19. Sherisse Pham, "How Much Has The US Lost From China's IP Theft?," *CNN.com*, 23 Mar 2018, https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html (accessed 14 Dec 2018).
20. Eswar Prasad. "China's Approach to Economic Development and Industrial Policy Testimony to the US-China Economic and Security Review Commission," *Brookings Institute*, 15 Jun 2011, https://www.brookings.edu/testimonies/chinas-approach-to-economic-development-and-industrial-policy/ (Accessed 14 Apr 2019).
21. Ibid.
22. Reggie Lai and Lingling Deng. "China's Industrial Policy and Its Implications for Foreign Manufacturers,"

American Chamber of Commerce in Shanghai, Legal & Policy, 8 Nov 2017, https://www.amcham-shanghai.org/en/article/chinas-industrial-policy-and-its-implications-foreign-manufacturers (Accessed 9 Apr 2019).
23. The White House, "Annual Intellectual Property Report to Congress," *WhiteHouse.gov*, February 2019, https://www.whitehouse.gov/wp-content/uploads/2019/02/IPEC-2018-Annual-Intellectual-Property-Report-to-Congress.pdf (Accessed 8 May 2019).
[24] Nicole Perlroth and David E. Sanger, "Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says," *The New York Times*, March 15, 2018, https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html?searchResultPosition=2 (Accessed May 10, 2019.)
[25] Dave Wagstaff, "He who has data is king," *embedded*, January 15, 2014, https://www.embedded.com/electronics-blogs/other/4427142/He-who-has-data-is-the-King (Accessed May 10, 2019).
[26] Geoffrey A. Fowler, "Alexa has been eavesdropping on you this whole time," *The Washington Post*, May 10, 2019, https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/?utm_term=.eafa554df6a1 (Accessed May 10, 2019).
27. Daniel Coats, "Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record to Senate Select Committee on Intelligence," *DNI.gov*, February 2018, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community (Accessed 19 Jan 2019), 19.
[28] "Mike Pompeo warns UK over Huawei 'security risks,'" *BBC*, May 8, 2019, https://www.bbc.com/news/uk-politics-48198932 (Accessed May 10, 2019).
29. Elisa Shearer, "Social Media Outpaces Print Newspapers in the US as a News Source," *Pew Research Center*, 10 December 2018, accessed via https://www.pewresearch.org/fact-tank/2018/12/10/social-media-outpaces-print-newspapers-in-the-u-s-as-a-news-source/ (Accessed 8 May 2019).
30. Jon Oltsik, The cybersecurity skills shortage is getting worse, *Cyber Security Office*, (January 10, 2019), accessed at https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html. (Accessed 8 May 2019).
[31] Jennifer Finney Boylan, "Will Deep Fake Technology Destroy Democracy?" The New York Times, October 17, 2018, https://www.nytimes.com/2018/10/17/opinion/deep-fake-technology-democracy.html?searchResultPosition=1 (Accessed May 10, 2019).
32. "Internet of Things - number of connected devices worldwide 2015-2025", *Statista.com*, March 8, 2019, https://www.statista.com/statistics/471264/IoT-number-of-connected-devices-worldwide/ (Accessed 8 May 2019).
33. David De Cremer, Bang Nguyen, and Lyndon Simkin, "The Integrity Challenge of the Internet-of-Things (IoT): On Understanding Its Dark Side," *Journal of Marketing Management* 33, no. 1–2 (January 2, 2017): 145–58, https://doi.org/10.1080/0267257X.2016.1247517. (Accessed 8 May 2019).
34. Berte, Dan-Radu. (2018). Defining the IoT. Proceedings of the International Conference on Business Excellence. 118-128. 10.2478/picbe-2018-0013.
35. Simone Cirani, Gianluigi Ferrari, Marco Picone and Luca Veltri, *Internet of Things: Architectures, Protocols and Standards.* (New Jersy: Wiley, 2019) 125.
36. "US Federal Cybersecurity Market Forecast for 2017-2022" *MarketSearch.com,* 4 Feb 2019, https://www.marketresearchmedia.com/?p=206 (Accessed 15 April 2019).
37. Natasha Singer, "Why the F.T.C. Is Taking a New Look at Facebook Privacy", *The New York Times.com*, 22 Dec 2018, https://www.nytimes.com/2018/12/22/technology/facebook-consent-decree-details.html (Accessed 8 May 2019).
38. "Privacy Laws, Regulations, And More", *General Service Administration*, https://www.thestreet.com/story/14536213/1/everyone-who-is-suing-facebook-for-cambridge-analytica.html (Accessed 8 May 2019).
39. "National Cyber Security Methodology," *National Cyber Security Index*, https://www.ncsi.ega.ee/methodology/ (Accessed 8 May 2019).
40. Ibid.
41. "ITU/BDT Cyber Security Programme: Global Cybersecurity Index (GCI), Version 1.0," *International Telecommunications Unit*, 28 February 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv3_documents/GCI%20V3%20Reference%20model.pdf (Accessed 8 May 19).
42. "E-identity," *E-Estonia.com*, https://e-estonia.com/solutions/e-identity/id-card/ (Accessed 8 May 19).

43. Donald J, Trump, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, *The White House*, 11 May 2017, https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ (Accessed 8 May 2019).
44. The White House, “Remarks by the President on Securing Our Nation's Cyber Infrastructure,” *The White House*, 29 May 2009, https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (Accessed 8 May 2019).