CLEARED
For Open Publication

Dec 12, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

25-T-0298

AY 2019-2020

Cyber Domain and Advanced Computing Industry Study (ES6762)

Col Andrew Nichols, USAF - Faculty Lead

CAPT Ramberto Torruella, USN - Deputy Faculty Lead

Seminar Members:

Ms. Stephanie C. Arnold, DOS, COL Mohammed S. Al Barazanchi, Iraq Army,
COL Jose A. Cora, USA, COL George I. Corbari, USA, Mr. Jeffrey A. Donnell, DIA,
Lt Col Jason M. Holcomb, USAF, Lt Col Christopher T. Johnson, USAF,
Mr. Daniel O. Joyce, USA, Mr. Sahan B. Kamara, DISA,
COL Aydin Kilic, Turkish Army, Col Amir Lazar, Israeli Air Force , CDR Mark A. Lindsey, USN
Mr. Andrew D. McClearn, DOS, Col Vladimir Milovanovic, Serbian Air Force
LTC Benjamin F. Sangster, USA, Mr. Antonio “T” Scurlock, DHS, Colonel Brent O. Skinner, USA
LTC Lance M. Sneed, USA, Lt Col Randolph B. Witt, USAF

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

The views expressed in this paper are those of the author and do not reflect
the official policy or position of the National Defense University,
the Department of Defense, or the U.S. Government.

Executive Summary

The Cyber Domain and Advanced Computing Industry Study team completed a comprehensive review of this industry by conducting engagements with over 30 organizations over a four-month period. Following these engagements, extensive classwork, and industry analysis, the study team developed this paper to document its findings and make a set of policy recommendations to strengthen the United States' position as a leader in the cyber domain and the advanced computing industry.

The rate of change in this domain is accelerating, and it is changing virtually every facet of our lives. Advances in quantum computing, neuromorphic chips, and artificial intelligence technologies, to name just a few, may enable a country to develop leap-ahead military systems that would make its adversaries' systems obsolete in a short time. Will the United States be the leader or be surpassed?

The United States retains its edge in many of these fields, but China and other countries are closing the gap. The industry study team analyzed and developed recommendations for over 40 issues, choosing to focus in this paper on the most pressing ones, those likely to manifest as crises with national security and profound economic implications in the next seven to ten years.

In Section 1, the paper opens with a blunt statement: The United States is under attack every day in and through the cyber domain and must, therefore, take bold action to mitigate and eliminate these threats. Section 2 pursues the narrative that our adversaries are seeking to diminish U.S. power and prestige through a campaign in the cyber domain and introduces the Congressionally-directed Cybersecurity Solarium Commission (CSC). The CSC studied the current state of cyber in the United States and reported its findings and recommendations organized around six "pillars," or functional recommendations, on March 11, 2020. There is a high correlation between the cyber industry study recommendations these six CSC pillars. This section also defines the Cyber Domain and Advanced Computing industry, which includes over 15 sectors. Four firms were selected for more in-depth study because they are industry leaders in the sectors most important to the Department of Defense (DoD) and other national security stakeholders. The results of these analyses are presented in summary, with detailed findings in Sections 3-6 and Appendix A, with the full firm briefings in Appendix E. Section 2 concludes with an assessment of the U.S. state of innovation, using a Massachusetts Institute of Technology (MIT) model of the innovation ecosystem.

The next four sections examine a set of challenges and conclude with policy recommendations, which the industry team recognizes come with a price tag. Veteran Pentagon policy and resourcing professionals understand that "Vision without funding is hallucination." Specific suggestions for resourcing these cybersecurity initiatives are found within some recommendation in this paper, while others are described more fully in separate policy memos written by the industry team. In addition, the team recommends that the Secretaries of Defense and Homeland Security dedicate 2% of their Fiscal Year 2021 budget request to resource many of the recommendations in this paper and those of the CSC.

Section 3 describes the workforce challenges facing the United States, including the acute shortage of skilled cyber domain workers. This section makes policy recommendation to include H-1B visa immigration reform and the expansion of apprenticeships and certifications to get more skilled cyber professionals in the workforce without requiring a four-year college degree. In order to increase our workforce resilience in times of crises, the section concludes with recommendation to create a civil cyber force, strengthen cyber reserve forces and initiate a cyberspace operations training corps (COTC).

Section 4 discusses a how the United States can maintain its global leadership in cyberspace and advanced computing by improving the cyber resilience of the nation. True national resilience includes the entirety of the public and private sectors. In order to achieve resilience, this section recommends cybersecurity education for all students, a national authority to oversee the 5G wireless implementation and the internet of things (IoT) to decrease our attack surface. Additional recommendations include

increasing remote or telework options for all workers and a digital counter information operations activity to disrupt adversaries' information operations campaigns.

Section 5 focuses on improving the security of the cyber ecosystem, with a focus on artificial intelligence, high-performance computing, the zero-trust network design, and promoting the growth of the cyber insurance industry. This section finds the United States' lead in quantum computing is at risk and explores how to better address vulnerabilities related to cybersecurity. It also includes a recommendation to implement an adaptive funding framework to give DoD the financial agility it needs for rapid software development.

Section 6 focuses on improving government collaboration with the private sector. Operationalizing cybersecurity inherently requires close collaboration to leverage commercial cybersecurity tools, private capital and technical skill sets from industry. The United States is at a disadvantage when compared to China's dominance of 5G hardware and its more agile approach to allocating radio frequency spectrum to 5G operations. To address this issue, the authors propose a government and industry partnership to develop open standards for the critical radio access network devices at the heart of 5G communications, and a proposal for a more open market and investment mode for the electromagnetic spectrum for 5G communications. Other recommendations include the strengthening of 5G collaboration with domestic and international partners.

Section 7 concludes the paper with a short summary. As critical elements in a coordinated, synchronized, and integrated cybersecurity strategy, the team's recommendations promote innovation and economic growth in the technology sector, improve the resourcing of U.S. and allied national security strategies, and create a more secure world for the United States and its friends and allies.

Appendix A discusses a central theme of the academic program at the Eisenhower School – mobilization – and, specifically for this industry study, what national mobilization means in the cyber domain, including how to mobilize NATO and other international partners. This appendix finds mobilization has historically focused on production of material for a kinetic war – but is not well suited for persistent cyber warfare. Many of the critical components that of cyber warfare systems are no longer made in the United States, which presents a challenge for increasing production to mobilize our cyber operations forces. The authors recommend the United States provide incentives for international computer component manufacturers to relocate or open new production facilities in the United States, similar to the incentives made to Toyota, BMW, and Mercedes to locate car production in the United States. And while NATO does not have robust cyber capability, several member states – notably Estonia – have developed significant cyber capabilities as a result of persistent gray zone warfare with Russia.

Appendix B provides an operational approach diagram, which describes our current state in cyberspace, the end state we desire, and how the recommendations in body of the paper support that end state. This diagram provides a one-page chart for senior and key leaders that allows them to visualize the recommendations of this paper, and which CSC Pillars and efforts they support.

Appendix C provides draft statutory language for three separate appropriations changes that would enact the Agile Funding Framework (AFF), and which would provide much-needed funding flexibility to effectively execute the acquisition flexibilities of the new Adaptive Acquisition Framework of DODI 5000.02. Enacting the AFF would enable DOD to implement the MIT Innovation Ecosystem Stakeholder Model, provide much-needed funding flexibility to supercharge research and development of IT, Cyber and software capabilities, and achieve funding efficiencies for these emerging capabilities.

Appendix D identifies the members of the ES AY19-20 Cyber Industry Study (IS) who contributed to this paper, along with a picture of each member and their respective follow-on assignments.

Appendix E contains the four Industry Analysis Briefs developed by sub-team members of the Cyber IS for the following corporations: Northrop Grumman Corporation, Microsoft, Verizon and IBM. These Industry Analysis Briefs directly informed the analysis and recommendations of this paper.

Table of Contents

Section 1: Introduction

There have been very few times in America's history that galvanized our resolve as citizens and united us closely as a nation. One such moment was December 7th, 1941, "a date that will live in infamy" according to President Franklin D. Roosevelt[1], when the Japanese Empire attacked the United States at Pearl Harbor, Hawaii. The attack killed 2,403 service members and wounded 1,178 more. On December 8th, 1941, President Roosevelt requested that Congress declare a state of war with Japan.[2] Another such moment was September 11, 2001, when terrorists attacked multiple targets in the United States killing 2,997, and several hundred more first responders have died since from related illnesses.[3] These "shock-event" attacks demanded and resulted in immediate responses by the United States.

Today, our country is under a different kind of attack. The enemy is not dropping bombs or launching torpedoes. Our present-day enemies utilize the ether of cyberspace to cloak their activity, providing near perfect anonymity while conducting long-term campaigns. They exploit the ever-expanding internet of things, our increased connectivity, and our individual ambivalence to leverage a *cyber war* against our country; conducting small operations over time, achieving alarming cumulative effects. The current fractured state of our political ecosystem provides a convenient distraction for our enemies carrying out these activities in cyberspace and complicate and delay appropriate U.S. response.

The United States has one of the most interconnected societies in the world. The U.S. economy and financial systems require connectivity. Public and private organizations rely on the internet to resource at least some portion of their business activity. These organizations, the internet, and the systems used to access the internet… are all part of the ***cyberspace ecosystem***. The word "ecosystem" gets its roots from ecology. It is defined as "a system, or a group of interconnected elements, formed by the interaction of a community of organisms with their environment."[4] Computers, computer scientists, internet service providers, the IoT devices… are all elements of the cyberspace ecosystem.

The cyberspace ecosystem of the United States is not well. While portions of it are thriving (e.g. connectivity...broadband service is available on a grand scale to almost anyone who desires it), other portions are in a desperate state requiring immediate attention (e.g. human capital...the United States is struggling to maintain a talent pipeline into technology-focused career fields). The security of the entire ecosystem is at risk. This may be best evidenced by the multi-billion dollar investments by our key global competitors in disruptive technologies such as quantum computing, which threatens U.S. asymmetric encryption practices designed to protect our private personal, commercial, and national security information. The United States must act immediately to begin the healing of our cyberspace ecosystem.

The recommendations in this paper are intended to help begin the healing process. The authors used the framework introduced in the 2020 Cyberspace Solarium Commission report as a guideline to shape the analysis and subsequent recommendations across various elements of the U.S. cyberspace ecosystem. In an era when U.S. national debt has surpassed $25 trillion, discretionary budgets are squeezed, and the nation faces a multitude of serious challenges, the industry study team recognizes these recommendations will not be implemented without substantial cost. That said, the costs of not taking action are even higher. Global cybercrime damages are expected to hit $6 trillion next year, continuing to exact enormous financial, operational, and reputational tolls on companies, organizations, and governments, comprising everything from corporate intellectual property to our national secrets.[5]

Section 2: Overview

The United States is facing significant challenges across all elements of national power by a rising China and a revisionist Russia seeking to restore its place amongst Great Power States. Although they possess near-peer capabilities, neither desires to engage the United States in armed conflict, so neither will engage in an activity so egregious that it sparks armed conflict. At the other end of the capability scale, North Korea and Iran, likewise, seek to undermine U.S. strategic advantages, and to do so without sparking a direct military response. Their motivation is further bolstered by the fact that they have no other options to challenge U.S. hegemony. In all four cases, our adversaries are using cyberspace to advance their agendas, engaging in campaigns of malicious activities below the threshold of armed conflict. Their objectives range from theft of intellectual property to undermining the U.S. political system and unity of the nation in the cases of China and Russia, respectively, to seeking to strike a blow financially or otherwise against the United States in a public and significant way for North Korea and Iran. The challenges facing the United States shake the very foundation of our nation's strength – the technological advantage of our economy and defense that have propelled us to greatness – is now unsecure and vulnerable. Additionally, these challenges have nullified U.S. dominance by removing combat power from the discussion, as each actor continues to engage in malicious activities in such a way that they do not spark or justify a kinetic U.S. response.

Over the past decade there have been growing concerns and calls for improved strategy to address these challenges. The Obama Administration released several publications, including a National Cyber Strategy and several Presidential policy directives, related to cyberspace security. The Trump Administration has continued along this path releasing its own version of a National Cyber Strategy and revising the Obama era directives in National Security Presidential Memoranda. Finally, the most recent and significant event has been the establishment of the Cyberspace Solarium Commission which studied the challenges in cyberspace before releasing its detailed March 2020 report outlining the framework for a continued and comprehensive evolution of U.S. National Cyber Strategy. The report identifies a number of areas (pillars) within which to organize and focus on robust and innovative ways to improve U.S. cybersecurity from the private sector to the interagency. Throughout this paper, our proposed recommendations will be linked to the CSC effort, expanding on the ideas and suggestions of this blue-ribbon commission of experts. The intent of the recommendations in this paper is to build upon CSC recommendations, not replace or detract from them. These linkages are summarized in Table 1 below.

Table 1: Crosswalk of CSC Pillars to Cyber Domain and Advanced Computing Seminar Elements

Cyberspace Solarium Commission Pillar Number and Title		Paper Section	Cyber Domain and Advanced Computing Seminar Elements
1	Reform the U.S. Government's Structure and Organization for Cyberspace	3	• Cyber Workforce • Immigration Reform • Apprenticeships • Cyber Reserve Force • Civil Cyber Force • Cyber Operations Training Corps
2	Strengthen Norms and Non-Military Tools	NA	No recommendations presented for this pillar
3	Promote National Resilience	4	• National Cybersecurity education • 5G and Internet of Things Authority • Promote telecommuting and remote work • Promote Information Integrity and fairness

Cyberspace Solarium Commission Pillar Number and Title		Paper Section	Cyber Domain and Advanced Computing Seminar Elements
4	Reshape the Cyber Ecosystem Toward Greater Security	5	• Adaptive Funding Framework for Rapid Software Development • Artificial Intelligence • Quantum Computing • Mobilizing National and Allied High-Performance Computing Resources • Accelerate Zero Trust Network Design • Cyber Insurance
5	Operationalize Cybersecurity Collaboration with The Private Sector	6	• Incentivize Open Radio Access Network investment for 5G • Agile Electromagnetic Spectrum Allocation and Management • Domestic and International 5G Cybersecurity Cooperation
6	Preserve and Employ the Military Instrument of Power	NA	No recommendations presented for this pillar

In the overview, we define the industry and its current conditions, highlighting the major challenges and business outlook and closing with the government roles and policies needed to strengthen these industries for national defense.

2.1 Industry Defined

The Cyber Domain and Advanced Computing Industry Study comprised the business areas and markets shown in Table 2 below.

Table 2: Cyber Domain Advanced Computing Industry Areas of Study [6]

- Enterprise Software/Applications
- Consumer Software/Applications
- Internet Media/Social Media
- Data Aggregators/Sellers
- IT Services
- IT Infrastructure
- High-Performance Computers
- Personal Computers

- Semiconductors & Processors
- Telecom Providers (Wireless & Fixed-Line)/Internet Service Providers
- Devices /Mobile Phones
- Autonomous Vehicles
- Human Capital
- Cyber Risk Insurance
- E-Waste Management

In the course of this industry study, the team had the opportunity to engage with industry partners in the United States as well those in Asia, Europe, and in Israel. The team also engaged with government agencies charged with defending U.S. interests in this industry. Senior leaders responsible for national security resourcing must work closely with large defense industrial base (DIB) companies, small start-ups developing a new disruptive technology, international firms, and academia to understand their challenges so we can work together to deliver solutions. The study team met this goal with numerous engagements summarized in Table 3 below. A more detailed list of firms and agencies studied by the industry study team, and where they fit in the cyber ecosystem, is found in Appendix E.

2.2 Current Conditions and Outlook

This industry study team examined the business sectors in cybersecurity, cyberspace operations and advanced computing, analyzing firms that are either market leaders or leading in investment and innovation in emerging advanced computing technologies. These firms were chosen because they were representative of other firms in this industry and had a strong presence in the industry sectors. Due to the COVID-19 pandemic, as businesses have closed or dramatically reduced operations, the overriding current state of the global economy remains in a downturn in many industries. In just two months, 10 years of U.S. job growth has been wiped out, as the Department of Labor reported 20.5 million jobs were lost in April 2020 and unemployment rose from 3.4 percent in February to 14.7 percent in April.[7] These new market conditions require continued collaboration between industry, government, and academia to help the U.S. economy recover. In many ways, this industry is doing better than most.

The paper now shifts to a summary of a more comprehensive analysis conducted by the industry study team of the four lead firms in Table 3 below: Northrop Grumman, Microsoft, IBM, and Verizon. This section also assesses the strength of innovation in the United States using MIT's framework.

Table 3: Cyber Domain and Advanced Computing Sector Firms[8]

Industry Sector	Lead Firm Analyzed	Additional Firms and Organizations Contacted
Cybersecurity & Cyberspace Operations	Northrop Grumman	Alion, BSA | The Software Alliance, Cisco, Crowdstrike, Cyber Threat Alliance, Defense Counterintelligence Agency (DCSA), DISA, FBI, ForgePoint Capital, IAI ELTA Systems Ltd., IBM, Illumio, Microsoft, Northrop Grumman, NSA, Palo Alto Networks, USCYBERCOM
Artificial Intelligence	Microsoft	BSA, Carnegie Mellon University, Facebook, Fujitsu, IBM, NVIDIA, The Software Alliance, University of Texas at Austin
High Performance Computing (Software & Hardware)	IBM	Applied Research Laboratories at the University of Texas ARL:UT, Fujitsu, Intel, NVIDIA, Rigetti, Texas Advanced Computing Center (TACC), University of Maryland Laboratory for Physical Sciences (UMD LPS)
Telecommunications (5G)	Verizon	Cisco, Intel, Taiwan Mobile, AT&T, CTIA

Table 4: Organizations & Firms Visited in Other Sectors [9]

Industry Sector	Other Firms and Organizations Contacted
IT Services	Northrop Grumman, Gartner, U.S. Patent and Trademark Office
Enterprise Software/Applications	CMU SEI, DoD CIO (DevSecOps)
Consumer Software/Applications	Alphalab, Microsoft Taiwan
Internet Media/Social Media	Facebook
IT Services	ITRI
IT Infrastructure	CISCO, Fujitsu
High-Performance Computers	IBM, NVIDIA, Fujitsu
Personal Computer	Microsoft
Semiconductors & Processors	Intel
Autonomous Vehicles	CMU National Robotics Engineering Center
Human Capital	CMU, University of Texas

Northrop Grumman Corporation (NGC) is a market leader in cyberspace operations and a major provider to DoD, with 83 percent of sales going to DoD and the intelligence community. Their past performance has been good, and they have strengthened their position in the space sector by acquiring Orbital ATK and the horizontal integration of cyberspace into all other product lines. The U.S. government has monopsony power over NGC, making the bargaining power of the buyer the most dominant of Porter's Five Forces. NGC derives its competitive advantage by its size and number of contracts with the U.S government. Their relationship with Orbital ATK caused Boeing to drop out of ICBM modernization, leaving the company as the sole source for this program that will span 20 years and at a cost of $85 billion. In its core markets, NGC is extracting greater value from suppliers by horizontally integrating them, yielding more revenue and increasing the security of their supply chain.

In the broader cybersecurity industry are competitors in friendly countries that are developing newer, more innovative solutions than NGC. The Israeli firm IAI Elta has done pioneering work in cybersecurity for aviation and cyber early warning and developed a training program to create a robust workforce of cybersecurity experts, a model that the United States should carefully explore to emulate these world leaders in the cybersecurity sector.

The Microsoft Corporation has been the industry leader in office productivity software and gaming since the beginning of the Information Age. Microsoft's goals today are to empower everyone to achieve more with Microsoft's software and services delivered through a secure cloud with AI integrated to help the human be more productive. Kai Fu Lee notes AI improves directly at the rate it is given structured data. Microsoft is advancing the integration of AI for office automation, with the aggregated (not personal) data collected from Office 365 users in the cloud. Microsoft's policy is not to track individual data, but to aggregate it for their AI to learn and provide more value to the customer.

Present and past performance has been very good, with the growth of Office 365 and Azure Cloud businesses. Microsoft is no longer focusing on selling exclusively its own product, and are now more likely to integrate other vendors' systems in a tailored solution, focused on trust and privacy between the customer and Microsoft. With this approach, they are distinguishing themselves from social media companies and Google, who are making money off consumer data, and are also leaders in AI research and development. The degree of rivalry and supplier power are the most dominant of Porter's forces. Competing with Microsoft's hybrid cloud with AI are similar offerings from Amazon, Google and IBM. Microsoft's competitive advantage is its known brand (leader in office automation for 40 years) and integration of its products with rival products for customers. Foreign competition is not a big challenge, though pirated software is. Microsoft is financially sound and is an innovative company with over 50,000 employees working in research and development of new products and services.

IBM's leading sector is cloud services and cognitive computing. IBM's mission is to transform companies from businesses informed by their data to a "cognitive enterprise" through the integration of AI and quantum computing in a hybrid cloud. Other sectors are not performing as well as industry giants like Amazon, Google, and Microsoft. IBM is a leader in innovation, with over 9,200 patents awarded in 2019. IBM's purchase of Red Hat for $34 billion signaled IBMs vision to be the leader in delivering hybrid cloud solutions and services to customers. The power of buyers and suppliers are the strongest of Porter's forces for IBM.

IBM differentiates itself with AI solutions for a cognitive enterprise and a very public R&D effort in quantum computing. IBM is investing in other quantum computing hardware and software researchers to use its quantum systems to advance state-of-the-art technology and applications, giving IBM a competitive advantage over smaller firms doing quantum research. IBM is also the company who built the world's fastest computer, called Summit. Foreign competition in high performance computing, including quantum computing, comes primarily from China. IBM's greatest risk is financial stability as their long-term debt to equity ratio is over 6.2. The COVID-19 economic downturn will likely lead to a delay in IT investments. IBM serves 95 percent of Fortune 500 companies, which may insulate it from the downturn to some extent and allows IBM to remain a leader in quantum technology development.

Verizon is the second largest telecommunications firm in the world and a leader in rolling out the critical 5G system in the United States. Their past performance in the evolution from 2G to 4G has been excellent, and they are poised to remain profitable as 5G, in conjunction with AI and advanced data analytics connected IoT, which changes the way we interact with the network and each other.

Verizon has the majority of 4G wireless market share in the United States, and is poised to continue that dominance in 5G. The greatest challenge for the United States is the competition with China on 5G rollout in allied countries, as China has lower prices on key 5G network hardware, raising concerns about the security of networks employing Chinese systems.

The four lead firms and other firms we studied undeniably possess cutting-edge capabilities and are leading in innovation. The technology sector in the United States is among the nation's strongest industries. In this respect, this industry is particularly well-positioned to support our National Security Strategy (NSS), the National Cyber Strategy, and to be mobilized in times of great need or crisis.

As this industry study team initially considered Atkinson's framework for assessing U.S. innovation, the U.S. business environment was very good and in its 10th straight year of growth. This environment is radically different now, as many companies are focused on keeping themselves out of bankruptcy as the U.S. economy contracts. The Congressional Budget Office projects GDP will decline by 12 percent in the second quarter, equivalent to an annual GDP decline of 40 percent. The adjustments that are needed in our innovation system are discussed in Section 2.5 below.

2.3 Challenges: Recession, Human Capital Reform, AI, and Great Power Competition

The U.S. government must modernize its antiquated human capital management systems to improve the identification, recruitment, development, retention and compensation of cyber talent. DoD is competing with the private sector for talented cyber professionals. Inflexible compensation and promotion systems act as a severe disincentive to government service. This human capital reform must also include a modernization of the immigration system to attract the best cyber talent worldwide, while restricting cyber education and training access to individuals that intend to return to our adversaries – with the know-how that U.S. institutions provided.

Many of these cyber workers will go to work on developing AI capabilities in industry and the U.S. government. Kai Fu Lee, a Taiwanese-born AI expert who previously worked at Microsoft and Google and is currently a China-based venture capitalist, points out that AI improves at the rate it is given large amounts of data, and China has an advantage due to its large population of connected users and lax privacy laws. The U.S. government will have to accelerate the employment of industry standard software development paradigms like DevSecOps and make structured data available for AI projects.

Finally, the United States must adapt its cyber strategies to confront our new world characterized by "Great Power Competition." China, Russia, and other adversarial nations increasingly undermine the interests of the United States and its allies in the cyber domain, including hacking our corporations, stealing our data and secrets, and positioning themselves to compromise our critical infrastructure on a moment's notice. Therefore, the United States must not only invest in key technologies to modernize U.S. cybersecurity, but also develop cyber offensive and defensive response policies that re-establish deterrence in the cyber domain. The United States and DoD in particular have long neglected the nuances and considerations of Great Power Competition in pursuit of warfighting capabilities and capacity under deterrence-based strategies. Those strategies are not effective in the current affairs of statecraft between the United States and near-peer adversaries.

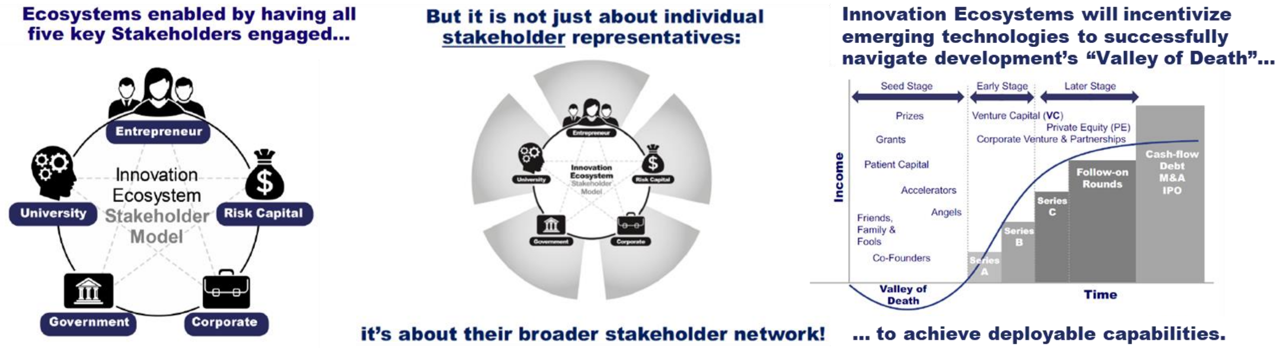
2.4 Government Goals and Role: Improved Cyber Policies and Modernized National Innovation System

As the President stated in the NSS, "Our fundamental responsibility is to protect the American people, the homeland, and the American way of life…We will protect our critical infrastructure and go after malicious cyber actors."[10] As a result, the primary goal of the United States in the cyber domain is to defend U.S. citizens and critical infrastructure from foreign adversary and criminal cyberattacks. The NSS promulgated four cyber principles to achieve cybersecurity: build defensible government networks, deter and disrupt malicious cyber actors, improve information sharing and sensing, and deploy layered defenses.[11]

The United States, however, remains "…dangerously insecure in cyber."[12] The root causes of the U.S. cybersecurity failure include: the lack of cyber deterrence cyber policies that allow the U.S. government to quickly respond to cyberattacks on the United States and its allies[13] and an innovation system that does not sufficiently incentivize the rapid development and deployment of new cyber technologies in the commercial and defense sectors.[14] Therefore, the role of the U.S. government is to fix these cybersecurity failures by implementing policies that re-establish cyber-deterrence, and to modernize the National Innovation System by incentivizing the delivery of cyber capabilities at the speed and agility required to defend the United States and its allies, its citizens, and its key infrastructure.

The United States has traditionally pursued classic *laissez-faire* economic policies which kept the U.S. government at arms-length from industry. Agile innovation and rapid deployment of defense cyber products and services, however, require an updated National Innovation System – a "network of institutions in the public and private sectors whose activities and interactions initiate, import, modify, and diffuse new technologies."[15] Rapid cyber innovation, therefore, requires increased collaboration between the government, academia, industry, technology entrepreneurs, and private sector risk capital – as illustrated below in MIT's National Innovation Ecosystem Stakeholder Model.[16] This modernized National Innovation Ecosystem will result in faster research, development, and deployment of emerging technologies within both the defense and commercial sectors.

Figure 1: MIT's National Innovation Ecosystem Stakeholder Model[17]


Ecosystems enabled by having all five key Stakeholders engaged…
Entrepreneur
University
Risk Capital
Government
Corporate
Innovation Ecosystem Stakeholder Model
But it is not just about individual stakeholder representatives:
it's about their broader stakeholder network!
Innovation Ecosystems will incentivize emerging technologies to successfully navigate development's "Valley of Death"…
Seed Stage
Early Stage
Later Stage
Prizes
Grants
Patient Capital
Accelerators
Angels
Friends, Family & Fools
Co-Founders
Venture Capital (VC)
Private Equity (PE)
Corporate Venture & Partnerships
Series A
Series B
Series C
Follow-on Rounds
Cash-flow Debt M&A IPO
Income
Time
Valley of Death
… to achieve deployable capabilities.

Section 3: Reform U.S. Government Structure & Organize for Cyberspace (Pillar 1)

Pillar One, Reforming the U.S. Government Structure and Organization for Cyberspace, is the foundational pillar for all the others. The inherent challenge in cyberspace operations is the lack of human capital cyber talent to meet the emerging threats and needs in the domain. In order to recruit and retain a pool of cyber talent, the government must institute changes in the form of immigration reform and other education and training programs recommended below.

3.1 Industry Sectors and Current Conditions

The cyberspace realm within the United States is comprised of, owned, controlled, regulated, and maintained by a number of different organizations including corporations, federal agencies, and state and local governments. The internet backbone is regulated by the federal government, its architecture is supplied by multiple corporations and relied upon by multi-national corporations who provide content as well as business and household consumers who increasingly rely upon it as vital to completing many different tasks in their everyday lives.

The workforce necessary to build, maintain and safeguard the architecture, and to conduct business in cyberspace is comprised of hundreds of thousands of individuals with myriad talents and skills spread across both private industry and government agencies. Private industry as well as state, local and the federal governments are facing a growing need for workers with skills and talent in cyber and cyber-related fields while at the same time the pool of workers being trained with these needed skills is not expanding at the same pace.

3.2 Challenges and Outlook

The United States faces a persistent shortage of qualified workers in computer science, computer programming, cybersecurity, and information technology, despite concerted efforts to develop America's science, technology, engineering, and mathematics (STEM) pipeline carried out over the past two Presidential administrations. President Obama's FY17 Budget requested $3.0bn across 14 federal agencies to help with STEM education.[18] President Trump followed up on these actions by issuing a Presidential Memorandum in September 2017[19] and by signing the Building Blocks of STEM Act in December 2019,[20] both of which were aimed at increasing STEM Education for K-12. Nevertheless, there are 918,000 vacant IT positions in the United States.[21] Absent additional efforts, the United States is projected to be short several hundred thousand if not millions of STEM workers by 2025.[22]

Specifically, with respect to cybersecurity professionals, according to the National Initiative for Cybersecurity Education (NICE) funded initiative CyberSeek, the shortage of cybersecurity professionals in the U.S. reached 314,000 by January 2019. [23] A joint 2018 Commerce and DHS report on the U.S. cybersecurity workforce concluded "the federal government depends heavily on its cybersecurity workforce" and "competition for qualified cybersecurity workers is intense across all sectors."[24]

This talent gap is exacerbated by a lack of skills of newly trained workers. Companies consistently complain graduates of cybersecurity programs lack the practical experience, fundamental knowledge, teambuilding, and communication skills required to be effective.[25] New hires require significant on-the-job training to effectively perform. A chief information security officer of a federal agency cited the commonly held frustration that the federal government provides excellent training and experience for new cybersecurity hires, who then leave for jobs with private firms.[26]

3.3 Policy Recommendations

Recommendation 3.3.1: Immigration Reform (H-1B Visas)

One possible means of filling this shortfall of workers is through immigration reform. Immigrants have long fueled the success of our nation's innovation economy. Nearly half of Fortune 500 companies were founded by first or second-generation immigrants, some of them former H-1B visa holders.[27] Today, many of America's top global technology firms – Microsoft, Google, IBM, and Adobe, to name just a few – are led by CEOs who first came to the United States as graduate students, got their first jobs through the H-1B program, and stayed on to make their indelible mark on America's tech sector and the overall prosperity of our nation.

The Immigration Act of 1990 established the H-1B visa program to help U.S. firms acquire human capital talent in specialized fields. The current annual H-1B cap, a statutory limit of 65,000 with an additional 20,000 visas available to foreign employees with advanced degrees from U.S. universities, is far below the annual number of company-sponsored H-1B petitions submitted, which totaled 201,011 in 2019.[28] The 85,000 annual H-1B opportunities is far below the number of international graduates from STEM programs at U.S. universities each year. According to the latest Student and Exchange Visitor Information System (SEVIS) data, which tracks foreign students in the United States, over 1.2 million international students were enrolled in SEVIS-certified U.S. schools, nearly double the total studying in the U.S. in 2006.[29] China has the most students studying in the United States with 377,070, followed by India with 211,700.[30] Most students from these top two countries are enrolled in STEM programs at U.S. universities.[31] In fact, 48 percent of all international students in the United States are in STEM fields.[32]

Congress should create opportunities for more of these STEM students to stay and work in the United States by increasing the H-1B visa cap from 65,000 per year to 185,000 per year. Additionally, the restriction of not counting the first 20,000 applicants who have a master's degree from a U.S. university should be replaced with an unlimited cap. This supplemental pool of H-1B visas could be subject to an additional $10,000 fee per visa to create a new source of federal funds – totaling $1 billion – to grow America's STEM pipeline and spur U.S. global competitiveness in high tech fields. An additional potential source of revenue would be the establishment of an auction based system for H-1Bs, an equivalent new visa category, or the underlying petition numbers that are in high demand by major tech employers.

Recommendation 3.3.2: Apprenticeships and Certifications

The United States has an apparent bias that requires workers to obtain a four-year college degree to be successful, especially in highly technical fields. To eliminate this bias and change the culture, policy should be promulgated to create a one- to two-year apprenticeship program, where individuals can become cybersecurity professionals without obtaining a four-year degree. The program would provide individuals with a technical defensive cyber operations degree and additional technical certifications. Such certifications as CEH, Security+, CISM, CISSP, to name a few, and other platform-specific credentials so the graduates can perform on networks upon completion of the program. The federal government and other institutions that adopt enhanced federal guidelines for cybersecurity training should offer additional internship and work-study opportunities for real-world experience to students from these programs.

The federal government should fund scholarships for cybersecurity training, competitively offering paid scholarships in return for a guaranteed period of service as a federal civilian, active duty military or reservist. Scholarship support and employment offers could also be awarded to winners of cyber competitions. Educational loan forgiveness in exchange for public service is another potential recruitment tool. The government could begin with a relatively modest scholarship fund of $5 million as a pilot project to increase recruiting. Reduced training costs would offset scholarship funds for those employees signing up for a guaranteed period of service. This option would help the federal government meet needs for entry-level personnel but is unlikely to solve long-term retention problems, as experienced personnel leave for higher-paying private sector jobs once their commitment to government service is up.

This accelerated and expanded cybersecurity pipeline would create a more substantial and faster program for cybersecurity professionals rather than a typical four-year degree. The result is a more specialized, highly trained workforce that can go directly into the government to assist in the public sector. This program is similar to a trade job such as in manufacturing but this pipeline specifically for defensive cyber operations. Germany has such apprenticeships for their trade skills and promotes industries with labor shortages early on, even as early as high school.[33]

Recommendation 3.3.3: Create a U.S. Civil Cyber Force and Strengthen Cyber Reserve Forces

The United States should build a strategic civil cyber force very similar in nature to the U.S. Civil Air Patrol. This congressional mandated, all-volunteer force could be called upon in the event of a national cyber incident.[34] Personnel would be trained through the proper channels and be available on call if needed by the federal government during national cyber incidents. The cyber force would be a combination of technical experts and cyber strategy professionals already possessing the appropriate level of security clearance and need-to-know who can provide immediate expertise in the event of a declared national emergency. This force could be built by offering free cybersecurity training to separating veterans or civilians willing to join a reserve component for a period of guaranteed service. Recruitment should emphasize the experience and training opportunities offered in the reserve forces which can be leveraged to gain lucrative private sector jobs.

Additional capacity would also be found in Cyber Reserve Forces that could be called upon to supplement federal government capability, especially in a crisis. The Cyber Reserve Forces could be placed under the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). The Reserve Forces would include industry professionals and subject matter experts, from civilian public and private sector talent. Their mission would include providing support to cyber missions in order to identify, protect, detect, respond, and recover critical infrastructure cyber assets. The forces would not participate in roles that require "direct" law enforcement or military engagement.

Because cyber reservists could support federal cybersecurity efforts remotely from their home units, cyber reserve units should be established in tech-heavy areas such as Silicon Valley, Austin or Boston to increase recruiting efforts and to facilitate easy service by personnel employed in the tech industry. This option creates opportunities to partner with industry, especially firms supportive of employing reservists. By providing training and practical experience in return for part-time service as a reservist, recruits would be available to fill cybersecurity positions in private firms. Cyber reserve forces offers a way for separating veterans to continue service, as well as those unable or unwilling to serve in the active duty force. The 2018 Commerce-DHS report on the national cybersecurity workforce identified veterans as available and underutilized in the cybersecurity field.[35]

Recommendation 3.3.4: Cyberspace Operations Training Corps (COTC)

The U.S. government needs to establish a whole-of-government, national program for cybersecurity education and development similar to ROTC--the Cyberspace Operations Training Corps (COTC). The COTC would be a long-term national education and development program that provides basic and advanced cybersecurity training and education at undergraduate institutions throughout the United States. The basic education would be standardized across all programs. Unlike ROTC whose sole mission is to produce military officers in uniform, COTC's mission would be to produce cyberspace operations professionals for the federal and state governments. The majority of COTC graduates would be non-uniform government employees (federal or state).

COTC would enable the U.S. government to execute the recommendations regarding Executive Order 13800. To build a COTC, Congress should appropriate sufficient funds in the current year's budget to: 1. Create a national level COTC leadership office; 2. Identify two to three undergraduate programs to stand up pilot COTC programs; and 3. Identify a federal department or agency to sponsor the programs. The establishment and resourcing of the COTC will provide the U.S. government with a long-awaited national level program capable of preparing, growing, and sustaining a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity.

Section 4: Promote National Resilience (Pillar 3)

The recommendations of the previous section centered around actions the U.S. government must take in the form of structure and organization to regain world leadership in cyberspace and advanced computing. This section continues to address how the United States can regain its world leadership in cyberspace and advanced computing by improving the cyber resilience of the nation. Nation refers to all components of the public and private sectors—the government, the people, private industry, etc. National resilience represents the third of six pillars of recommendations produced by the CSC to reduce the "probability and impact of cyberattacks of significant consequence."[36] Implied in this statement is the understanding that stopping all cyberattacks is a futile effort, but a national resilience will enable the United States to fight through cyberattacks and recover quickly to minimize their impact. The CSC's definition of resilience as "the capacity to withstand and quickly recover from attacks that could compel, deter, or otherwise shape U.S. behavior,"[37] explains this impact and its implications. This resilience is crucial for cyberspace deterrence by increasing the cost of cyber actors through hardening of the U.S. attack surface and limiting the pay-off of cyberattacks through a speedy recovery.[38]

4.1 Industry Sectors and Current Conditions

The relevant sectors of the cyber and advanced computing industry related to promoting national resilience span the industry's entire gamut. Each sector plays a role in promoting national resilience from telecommunications providers, to e-commerce and security companies, to software developers, cloud providers, and hardware manufactures just to name a few. This large span stems from the biggest challenge of resilience—scale—addressed in the next paragraph. U.S. national resilience as it stands now is poor as evidenced by the growing attacks and threats from cyber actors (representing the absence of deterrence due to a lack of resilience), the continued crippling of various local governments and organizations from malware, such as ransomware, and the success of foreign digital influence or information campaigns sowing seeds of doubt in the U.S. political system.

4.2 Challenges and Outlook

The real challenge in national resilience is the scale of the effort. As mentioned before, a true national resilience includes the entirety of the public and private sectors. Focus on particular areas, populations, or sectors just leaves the unfocused spots that much more vulnerable and attractive for cyber actors—thus rendering any narrow resilience efforts worthless. Too much focus in particular areas is akin to the French buildup of the Maginot Line following the end of World War I. Rather than face the potential high costs with an assault through the heavily defended Maginot Line, Nazi Germany pursued the much less fortified route through the Netherlands and Belgium to get to the same end result—an invasion of France. A perpetual cycle exists between the advancement and implementation of new technology and the corresponding actions needed to evolve the national resilience in order to keep up with these advancements. This makes the national resilience, and the efforts associated with bolstering it, a continuous investment to make it an effective deterrent.

Without a strong national resilience, the United States remains an attractive and fertile target across the spectrum of cyber actors from state-actors to cybercriminals and terrorist organizations to hacktivists. U.S. leadership in cyberspace and advanced computing will continue to erode under this constant barrage and threaten its national security, economic well-being, public health and safety and the confidence in its democratic political system.[39] The following recommendations only begin to scratch the surface. This is an incredibly difficult challenge and much more effort and study are necessary to reach the lofty goals of U.S. national resilience as a cyber deterrent.

The outlook of resourcing national resilience efforts is a current a bit bleak. Some of these recommendations could prove quite costly. One way to initially fund these efforts as well as incentivize national resilience across the nation is to fine organizations and companies for data breaches. Victims of data breaches often pay a price with losses in customers, remediation actions, and increased security efforts, but what if they also had a pay a fine based on the size of the breach and the negligence related to the cause. There are many, many details to flush out through further research but a fine system for security lapses could provide the resources needed for these recommendations and well as the incentive for all parties to make resilience a higher priority.

4.3 Policy Recommendations

Recommendation 4.3.1: Cybersecurity Education for All Students

There are many efforts in the public and private sector aimed at building out the U.S. cybersecurity workforce. This is incredibly important work to thwart current and future cyber threats, but all these efforts are aimed at identifying, preparing and/or developing the workforce that will serve as cybersecurity professionals. This policy recommendation works to raise awareness, understanding and knowledge of all citizens, not just those targeted to be cybersecurity professionals. Doing this increases the cyber resiliency and security of the nation, businesses, and citizens in the face of current and future cyber threats. In the 1950's, the United States faced an existential threat from the nuclear-armed Soviet Union. To help the population prepare for a nuclear attack, but more importantly, realize the seriousness of the threat, schools across the country instituted "duck and cover" drills. The effectiveness of these drills against a nuclear weapon remains suspect at best, but these drills did a great job of training and educating an entire generation of American students about the seriousness and possibility of a nuclear attack. The duck and cover drills of today are not about nuclear war; rather they consist of a cybersecurity education program combining the realization of the seriousness and possibility of cyber threats with knowledge, skills, and experiences to combat or stymie them.

This policy has a short-term goal of increasing the cybersecurity awareness, understanding and knowledge of all U.S. school-age children and teenagers. This is a necessary step to feed the long-term goal of having a cybersecurity-literate population that is much less likely to be the weakest link in the defense and protection of our information and data. This recommendation implements a cybersecurity education program at every level of primary and secondary education, or at the first level schools expose students to electronic devices in the classroom. Similarly, teachers will be trained in cybersecurity to teach the fundamentals as part of their regular curriculum. Each school district will have at least one fully certified cybersecurity professional to provide teachers with currency training as well as provide more advance cybersecurity classes as appropriate. This could be a new hire or an existing staff member completes the necessary training and certification. Students' grasp of cybersecurity will be part of standardized testing against a national standard provided as part of CISA's curriculum development. Successful completion of a basic, grade appropriate, cybersecurity awareness certificate is also a requirement to matriculate to the next grade.

Recommendation 4.3.2: 5G and IoT Authority

This next recommendation is to establish a single 5G and IoT Authority in order to "accurately and comprehensively understand, asses, and manage risk" across this pivotal new part of the cyberspace domain.[40] Attacks on the virtual domain are not new, but their power and danger are increasing. Entering the world of 5G will only enhance connectivity and therefore increase the attack surface available to cyber actors. Therefore, risk and the expansion of 5G technology increases the potential scope of attack by malicious agents. This will result in the proliferation of digital products that are vulnerable to attack, as well as cause the development of a wider range of malicious assault tools.

The leap in networking capabilities from 5G will bring a new world of connectivity between physical entities and the cyber domain from IoT to Massive Internet of Things (MIoT), through smart cities, autonomous traffic and robots. 5G technology will affect every aspect of life in the United States and around the world. It will change the way industry, government, municipalities and others work. 5G will also allow a leap in AI-based automation, which will increase the scope of core processes that do not involve a human hand. Since AI is mostly based on software developments, the AI ecosystem adds to the potential for vulnerability in the form of security breaches and software-level manipulations. All the above indicate a need for a different security approach and a whole-of-nation effort**.** This includes imposing manufacturers' responsibility on the security level of their products, regulating development processes, and subordinating methodology to all innovation processes.[41] This effort will require budgeting and other government support to enforce security standards on small manufacturers as well.

A national authority for IoT and 5G must be established to bring together the leading forces in the 5G market. The Authority will include at least DHS, the Department of Commerce and National Institute of Standards and Technology (NIST) has an important part in the industry standardization and its deliverables need to be mandatory not only for the federal agencies, DoD (USCYBERCOM), private industry (Verizon, AT&T, etc.) and academic representatives. The U.S. government must establish a set of laws that standardizes and regulates the 5G network and IoT. It is also necessary to establish a federal regulatory mechanism for law enforcement. The long-term goal should be a 5G network secured by cyber-protected products, a reliable hardware supply chain, and connectivity with encryption capabilities and compartmentalization.

The world is entering the Second Machine Age, where the 5G network and IoT will form the basis for the information revolution. Only a synchronized national effort will allow the United States to lead innovation in 5G on the one hand and protect national interests and security from cyber-attacks on the other. The new authority will require a relatively short period of time to complete the framework that will address the challenges and then to implement the U.S. strategy for 5G.[42]

Recommendation 4.3.3: More Remote Work Options

Along with the advancements 5G will bring, a new economy will develop to harvest, manage, and sell the information 5G-based systems will need to support data-intensive applications so they can perform at their optimal levels.[43] The changing landscape of this future economy demands greater flexibility for labor, less reliance on expensive brick and mortar office locations, and the ability to accommodate increased reliance on “gig workers” who focus on specific tasks for short periods of time. The COVID-19 pandemic demanded the DoD and other elements of the interagency continue to function with a large portion of its workforce completing tasks remotely, working virtually alongside teammates. Faced with the reality it is indeed possible to accomplish a significant portion of DoD tasks remotely, it is time to assess the value proposition of a remote workforce supporting the DoD. Such a workforce enhances resiliency by dispersing the workforce making it less susceptible to a variety of impacts from weather, communicable disease, to natural disasters and attack. Additionally, the benefits of a dispersed workforce reduce the cost of physical structures and offices, allowing employees to live in lower cost cities, and reduce traffic in areas with major military/DoD populations. To achieve these benefits DoD and USG will need to invest significantly in cybersecurity and the federal government will need to invest more in national high-speed networking capabilities. These investments will also benefit the private sector who will follow the government lead toward more efficient ways of employing their workforce to innovate, design, administer, and produce products and services for the digital age.

Recommendation 4.3.4: Digital Counter Information Operations

In perhaps the greatest imperative of our time, it is necessary to address the relentless propagation and reproduction of disinformation, fake news, and blatant manipulation of the American public. As American citizens, we value rights of a free society—first among them is the right to free speech. While we have a history of tremendous tolerance and latitude to the expression of ideas, there are restrictions on free speech. One cannot yell fire in crowded movie theater or make verbal threats of harm against another person. In the same way, it is unlawful to bear false witness, to lie to a law enforcement officer or in Congressional Testimony. In the United States, we value truth and the rule of law. In recent years, adversaries have taken advantage of our open and tolerant systems to inject false narratives, misinformation, disinformation, and fake news to foment discord and influence not only public opinion but the inner-workings of the U.S. government at the highest levels. While not recommending a government supervised, driven, or endorsed plan to censor or limit speech, we recommend requirements to attribute news stories and validate the identity of those promoting news or stories, legitimate or not. For news agencies, politicians, and others who make a habit of promoting false narratives and misinformation, their punishment should not be incarceration or other sanctioned punishment, rather it should be public shame as they are exposed. For the adversaries who peddle in such malicious behavior, they should be subjected to the full power of the U.S. government in terms of counter-espionage, criminal prosecution, and counter-information campaigns by DoD Cyber Mission Forces. We are not advocating the suppression of free speech, rather we are recommending that greater value be placed on factual and responsible reporting, and that adversaries who promote false narratives against the interests of the United States experience consequences for their actions.

Section 5: Reshaping the Cyber Ecosystem Toward Greater Security (Pillar 4)

Pillar 4 of the CSC Report implores the U.S. government and its allies to reshape the cyber ecosystem for greater security.[44] This effort will require "[r]aising the baseline level of security across the cyber ecosystem" to "constrain and limit adversaries' activities [in the cyber domain]."[45] Doing so will require close collaboration with industry, since "the vast majority of this [cyber] ecosystem is owned and operated by the private sector."[46] Additionally, emerging technologies such as artificial intelligence (AI), high performance computing (HPC) and systems architectures like zero trust (ZT) have the potential to dramatically increase cybersecurity and provide insurmountable capabilities in weapons systems and other platforms.[47] The danger, however, is if our adversaries develop them first, they stand to gain insurmountable capabilities over the United States. Because some of these emerging technologies have a long-term research horizon before they will produce commercial products, they may be less attractive investments for the private sector. As a result, and as the CSC Report recommends, for these key, potentially disruptive technologies, "the U.S. government must explore legislation, regulation, executive action, and public-as well as private-sector investments."[48]

Although the cyber ecosystem has seen tremendous progress, it has opened a plethora of opportunities for our adversaries to exploit novel vulnerabilities ranging from cyber-espionage to surpassing us in certain emerging technologies. Absent swift proactive steps, the United States will remain vulnerable to increasingly sophisticated attacks designed to interfere in our cyber domain, steal our data and secrets, weaken our military capabilities, undermine our democratic institutions, and encroach upon U.S. corporate competitive advantages. This section explores how we can protect our national security, promote our economic prosperity, and retain U.S. leadership in cyberspace by modernizing its funding constructs via the Adaptive Funding Framework (AFF), promoting a larger, more mature cyber insurance market, and effectively investing in the capabilities of AI, HPC, and ZT.

5.1 Industries – AI, HPC, ZT, and Cyber Insurance

Advances in analytics and "big data" are helping AI users provide a level of speed and accuracy not previously seen. Developments in AI will continue to author new infiltration techniques from our adversaries looking to breach data security protocols in governmental and commercial organizations. This digital explosion has ushered in a new wave of threats, which must be addressed through both offensive and defensive cyber operations. These cyber tactics will not be possible without ample resources dedicated to the entire cyber ecosystem. One means of protecting organizations against this increased volume of cyber threats is with cyber insurance. Still a developing industry, it has the potential to promote cybersecurity best practices, while protecting organizations from cyber risk.

Within the field of HPC, quantum computing (QC) is remains very nascent, but offers enormous transformational potential with "disruptive possibilities [that] far exceed that of any technology since nuclear weapons."[49] With its vastly superior capability and speed over any supercomputer that exists today, QC is expected to power major advances in virtually every field. Because this may be more than a decade away, the U.S. must position itself to succeed over the long-term in QC "not only to reap [its] benefits...but also fortify an internet of classical computing devices to survive an era of quantum threats."[50] Meanwhile, as government, the private sector, and academia explore potential applications for QC, the broader field of HPC is continually delivering new capabilities.

ZT offers a different approach to cybersecurity. From the time it was first launched as a concept to today, many vendors have initiated research, development, and implementation of their own solutions. It is not always evident whether they approach the same concept in different ways or if there are substantial differences in their offerings that can lead to diametrically opposite solutions. One thing is for sure, ZT has led to new ways of building a systems architecture and an entirely new mindset.[51]

5.2 Current Conditions – Potentially Catastrophic Vulnerabilities in the Cyber Domain

For more than 20 years, our adversaries have enlisted the use of cyberspace to undermine the American way of life. The United States, however, is still not armed with the necessary speed and agility to comprehensively defend this nation and its allies in cyberspace. Combined efforts to improve must begin with (re)building a resilient cyber ecosystem, one which intertwines deterrence, detection, response, and use of capabilities to ensure our national security. Although the cyber domain has come with economic growth, technological dominance, and improved quality of life for nearly every American, it has produced an array of dilemmas centered on security, privacy and ethics. As Americans create an abundance of connections through the digitization of information, products, and services, our foes have seized on these very opportunities to disrupt critical infrastructure, damage economic and democratic institutions, and uproot our systemic trust in the security of information. As we continue to conduct operations in the cyber domain, we require levels of data security, resilience, and trust that neither the public nor private sector is currently prepared to provide. Even as we continue to raise cybersecurity and encryption standards and protocols within our organizations, our adversaries are finding gaps within third parties and vendors that will create ripple effects throughout every one of our supply chains.

The United States leads the world in emerging technologies like QC, however this preeminent position is threatened by China, which, after a late start, announced an $11.4 billion investment to be the world leader in QC by 2025.[52] To date, U.S. government funding for QC research has been sporadic and lacked coordination.[53] The National Quantum Initiative Act, enacted by Congress on December 21, 2018, is a good start toward changing that. The Act aims to set goals and priorities for a 10-year plan and came with $1.275 billion for research to accelerate scientific breakthroughs in the technology.[54]

5.3 Challenges – Enhanced Paradigm Required to Secure Cyberspace

The current cybersecurity approach can metaphorically be described as defending a castle by encircling it with high walls and a moat with the occasional drawbridge to allow well-meaning guests to cross and keep bad ones out. But if a bad actor gets past the moat, he has the keys to the entire castle. The United States needs a new cybersecurity paradigm. The current approach is inadequate to fulfill its purpose, protecting against the ever-increasing onslaught of bandits disguised as good guys, who easily penetrate the castle wall. This poses an unacceptable risk, including to U.S. national security.

The causes of these security vulnerabilities include the increased number of participants in cyberspace, which, unlike in previous times, is much larger and far beyond the main control unit and storage space. Moreover, access is provided remotely through multiple devices such as mobile phones, tablets, computers, applications, public and private clouds, databases, the IoT, sensors and the like – all with different vulnerabilities. As a result, the boundaries between external and internal (defended) cyberspaces are being lost. Trust in the cyber network has become a critical principle in work and communications. For these reasons, we need a new or improved cybersecurity paradigm that will protect individuals, the nation, and our allies. The enhanced approach will also need to leverage the capabilities of AI, HPC, and ZT to more effectively protect U.S. national security.

5.4 Outlook – Great Power Competition Race to Develop AI and HPC

While the U.S. remains at the forefront of these emerging technologies, the seemingly – while likely not actually – unlimited resources behind state-backed initiatives in China pose the greatest threat to continued U.S. dominance. This is especially true as the U.S. national debt soars and our economy falters during the COVID-19 pandemic. These markets are all poised for continued innovation and growth, but in an era of declining U.S. government discretionary spending, advances will increasingly rely on effective collaboration between government, industry, academia, and our international allies. Pooling our talent, resources, and innovation ecosystems will be critical to our collective security and economic prosperity, which depend on preserving our lead.

5.5 Government Goals and Roles – Incentivizing Basic Research for AI and HPC

As recognized since NSC-68,[55] the U.S. "center-of-gravity" is the prosperity of its economy, which allows the U.S. to allocate significant resources to defense. As a result, continued economic growth and technological innovation are core U.S. policy goals. Technological innovation, particularly for defense products and services, requires a "network of institutions in the public and private sectors whose activities and interactions initiate, import, modify, and diffuse new technologies."[56] In the new "knowledge economy," rapid cyber innovation necessitates increased collaboration between the government, academia, industry, technology entrepreneurs, and private sector risk capital. A modernized National Innovation Ecosystem will result in faster research, development and deployment of emerging technologies within both the defense and commercial sectors.

In the emerging industries of AI and HPC, it may take decades to yield commercial products that recoup private sector investment, causing firms to be hesitant without a clear, positive government signal. Yet these technologies are potentially so transformative that the nation which develops them first may gain an insurmountable lead. As a result, the U.S. government's role must be to support positive externalities and correct any market failure of underinvestment by flexibly funding the basic long-term research that will lead to the development and ultimate deployment of AI and HPC capabilities in our commercial, defense, and cybersecurity ecosystems. There is also a role for the U.S. government to promote a larger and more mature cyber insurance industry, which will lead to enhanced cybersecurity practices and more robust data sets, which are critical for building risk models and pricing. The following policy recommendations describe these in greater detail along with implementation steps.

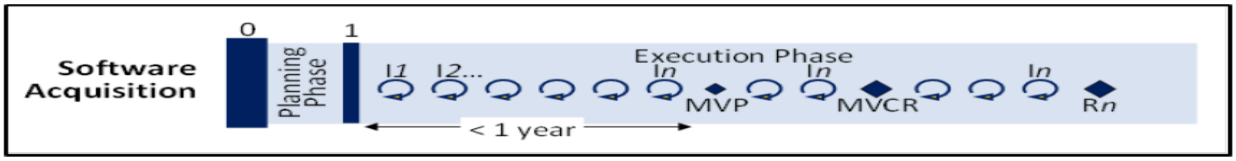
5.6 Policy Recommendations and Implementation

Recommendation 5.6.1: Implement the Adaptive Funding Framework (AFF)

On January 23, 2020, the USD (A&S) instituted dramatic policy reforms to the DOD Acquisition System, termed the "Adaptive Acquisition Framework" (AAF).[57] The AAF streamlined the traditional "waterfall" acquisition system to an "adaptive" acquisition system that could deliver faster acquisition performance for the acquisition of Information Technology (IT) and software.[58] The AAF, however, will not achieve the speed of acquisitions in IT desired by DOD without an equivalent congressional reform of the sequential “Waterfall Funding Framework” (WFF) towards an *Adaptive Funding Framework (AFF)* for IT, software and cyber.

The AAF for software acquisitions envisions a process of “iterative delivery of software capability… and iterative deployment of capabilities to the operational environment.”[59]

Figure 2: DODI 5000.02 Software Acquisition Pathway



The current WFF (RDT&E-Procurement-O&M), however, cannot support the AAF’s software acquisition pathway, since it is a “sequential waterfall.” To empower the AAF’s iterative IT development and a National Innovation Ecosystem for AI, HPC, ZT and more, DOD needs funding flexibility via three proposed appropriations modifications to create the AFF: (1) a “cradle to grave” Cyber/IT Appropriation (C/ITA); (2) unprogrammed “RDT&E, Other” for IT/Software/Cyber; and (3) inclusion of RDT&E efforts in the Expense/Investment Threshold Authority (*See* Appendix C for Draft Statutory Language).

Recommendation 5.6.2: Build our Artificial Intelligence (AI) Ecosystem

The promise of AI, and the endless possibilities for future innovations, can be seen through the prism of "big data" processing and machine learning. In that same breath, we seem to forget the importance of AI within the cyber ecosystem, which will be a crucial component in defending future attacks from our adversaries, who are continually seeking technological breakthroughs in efforts to weaponize AI to the detriment of humanity. Our adversaries, however, are also eyeing undetectable and sophisticated malicious codes to destabilize the cyber domain through a set of "offensive" AI tactics in attempts to compromise our organizational critical and key infrastructure systems. The United States must respond with a "defensive" AI posture whose purpose is not only in defense of cyberattacks, but whose AI actions includes a close-knit partnership between humans that incorporates American ethics and domestic and international standards on the use of forced AI.

This change will not happen until the United States spends sufficient resources on a currently immature cyber ecosystem that takes inventory and develops "a skilled workforce; the digital capability for capturing, handling, and exploiting data; and the technical foundation of trust, security, and reliability."[60] The demand for an organizational structure, comprised of the necessary skill sets and systems, is essential before introducing AI-related changes within the government. A 2019 RAND study noted that the "difficulties associated with verification and validation of AI capabilities, particularly learning algorithms, will require the workforce adopting AI to be comfortable with processes and standards that are a complete departure from normal DoD practice."[61] DoD must continue to advance its efforts by partnering with industry and academia while addressing the criticality of data resources through additive data protection, sharing, and analysis. The United States must be adamant in incorporating AI technologies into future systems and processes – to include weapons. In doing so, the DoD must discover those methods which minimize “unintended biases” in emerging AI systems and processes. Considering these “unintended bias” condition indicators, the United States must mitigate, as the DoD develops AI systems with national security applications.

These skillsets are not organic to DoD, as "many digital innovation skill sets do not match with existing career tracks."[62] DoD is looking for new policies that allow the government to hire employees from the business sector at specific ranks, bringing in those skill sets. A March 2017 study from the Task Force on Defense Personnel recommended that we "allow individuals with noncombat-specific skills (e.g., acquisition, cyber, finance, engineering, medical, law) to enter the military at higher ranks."[63] DoD must implement this recommendation to fill critical knowledge gaps within DoD.

Recommendation 5.6.3: Expand and Sustain Federal Funding and Partnerships in QC

New frontiers in HPC will allow us to solve a multitude of problems that are currently unsolvable, from unlocking cures for today's incurable diseases to revolutionizing how we encrypt our national secrets. However, experts say it may be 20 to 30 years or longer before the capabilities of QC are fully realized. This time horizon and the prospect of never realizing tangible gains disincentivize private investment, making federal support all the more essential, particularly for basic research.

To maintain its edge in QC and associated technologies, the United States must further increase and commit to consistent, long-term federal funding, establish the world's premier national research center dedicated to quantum information science (QIS) and QC, and expand and integrate domestic and international partnerships in the QC ecosystem. The National Quantum Initiative Program (NQIP) offers an exciting opportunity to bring leading research by U.S. corporations, universities, and national labs under a more centralized, coordinated endeavor, and to expand international cooperation with like-minded governments and foreign industrial partners already investing in their own quantum initiatives.

Congress should appropriate an additional $5 billion in FY2021 funding for the NQIP to establish the national quantum research center and support the most promising practical applications of QC and continued advances in QIS, which has already produced measurable gains and will help to bridge the progress gap until QC bears fruit. This increase in funding, combined with continued investment by the private sector and partnership with our allies, will bring the U.S. QC research budget closer to what is currently a tenfold higher investment in QC by China. The National Quantum Coordination Office in the White House Office of Science and Technology Policy (OSTP) would oversee and coordinate partnerships with industry and academia, and the Department of State would engage with our allies. Only by leveraging our collective talents and resources will we maximize the value and impact of our investments, secure our national interests, and effectively compete with China in this space.

Recommendation 5.6.4: Mobilize National and Allied HPC Resources

While the quest for quantum supremacy continues to unfold, significant advances in the area of HPC are unleashing exciting new capabilities every day, ready to be harnessed for national security objectives. This recommendation seeks to institutionalize the current COVID-19 response mechanism of bringing together private-public efforts spearheaded by OSTP. The current effort builds on the NSF-funded Extreme Science and Engineering Discovery Environment (XSEDE) cyberinfrastructure program, to be able to rapidly scale computing resources. We recommend creating a reserve contract mechanism that can be activated via DPA to dedicate additional private sector high performance cloud computing resources for national security during a crisis, in order to facilitate both surge and full mobilization of computing resources. This would establish a contractual relationship for the long-term between the federal government, industry, and academia. The contract mechanism would agree on accessibility timelines, supporting manpower needs, quantified computing resources, and cybersecurity baselines, and the USG can put together these cyberinfrastructure mobilization contracts with minimal funding, subject to surge needs. During the COVID-19 crisis, the XSEDE program has been utilized by OSTP as the contractual framework, with participants such as IBM, Microsoft, Amazon, Google, Intel, NVIDIA, Department of Energy national laboratories, NASA, all NSF-funded national data centers, and all of the major high-performance centers in U.S. academic institutions.[64]

While the COVID-19 effort is voluntary and restricted to researchers looking for vaccinations, therapies, and cures to a variety of problems associated with the disease, our recommendation is to create a contract mechanism that greatly expands the potential applications available to the U.S. government that would use super computing resources. These might include new weapons program applications, biotechnological discoveries, and information war methods in a hostile confrontation with one of our great power rivals. The activation of any of the line items of the contracts would be subject to mobilization needs. The U.S. effort would be accompanied by the creation of an agreed upon framework for activating and protecting international components of U.S. and allies' computing networks.

Recommendation 5.6.5: Accelerate Zero-Trust (ZT) Network Design

ZT is a concept that has long preceded the term "zero trust." Its underlying concept of "de-parameterization"[65] offers a different approach to cybersecurity, not merely safeguarding the perimeter of a system, but establishing and embedding granular authentication and authorization throughout the system's architecture. It treats all cyber domain entrants as a potential threat. Once a user is authenticated and authorized, access is permitted for that session only. ZT is an architecture that applies not only to individuals, but also all kinds of devices, including computers, sensors, and the IoT.

DoD should take the lead and influence the further development and standardization of ZT to meet the enhanced security needs of our cyber ecosystem. Currently, many vendors offer niche solutions, but none offers a single, comprehensive one. [66] DoD and other federal agencies would benefit from a more standardized ZT solution that is not dependent on a single vendor, which may also lead to vendor "lock-in" and interoperability issues. DoD should, however, collaborate with industry partners in developing core industry standards that will promote the development of ZT in the defense and commercial sectors. Until ZT industry standards are developed, DoD could internally adopt a hybrid or advanced phased implementation model. Within the phased development and implementation, DoD should also incorporate technologies and innovations such as AI and AC to support ZT development.

Recommendation 5.6.6: Promote the Growth and Maturation of the Cyber Insurance Industry

Cyber insurance has been available for decades, with interest spiking around Y2K and the 9/11 attacks[67] and more recently after cyberattacks on prominent firms, organizations, and governments, which have exacted enormous financial, operational, and reputational tolls. The average data breach costs $3.9 million,[68] and experts predict total global cybercrime damages will hit $6 trillion next year.[69] Although recent high profile attacks have increased demand for cyber insurance, now a $2.4 billion industry with a 7.8 percent annual growth rate,[70] it remains an immature market in which data and analytics are lacking.[71] Data allows insurance companies to create risk models critical for measuring and monitoring their accumulation of risk, pricing, and securing reinsurance coverage. "In the absence of risk transfer mechanisms, the financial cost of major cyber incidents will [continue to] be borne by governments, [corporations,] and their shareholders."[72] The cyber insurance industry also lacks standards and suffers from adverse selection with the more at-risk organizations seeking coverage.

A larger cyber insurance market offering incentives for premium discounts would promote a proliferation of cybersecurity best practices. Various policy interventions by government could remedy the growing pains of this burgeoning industry and champion the use of this tool that helps organizations mitigate cybersecurity risk. Legislation and government policies such as mandating cyber insurance for certain industries or to win government contracts[73] also offer a means to solve the adverse selection problem and increase the availability of data. The federal government could also set industry standards and aid in the collection of valuable actuarial data by creating a cyber incident data repository and requiring the submission of that information. As a supplemental benefit, the federal government may be able to raise revenue by charging a fee for services it provides to industry, for cybersecurity certifications, or a levy on cyber insurance premiums, which could fund other cybersecurity initiatives.

Section 6: Operationalize Cybersecurity Collaboration with Private Sector (Pillar 5)

Private industry develops many of the technologies the U.S. government relies upon for critical national security missions. The DoD and other agencies must establish strategic partnerships with U.S. companies to help align private sector R&D resources to priority national security applications. As discussed in the previous section, the private sector is a large majority of the cyber ecosystem, driving the importance of CSC Pillar 5, *Operationalize Cybersecurity with the Private Sector*. Compared to the government-funded R&D of the past, today, industry has taken the lead in cybersecurity innovation expertise. This has led to adjustments in how the U.S. government must develop national strategies that incorporate the critical technologies required to remain dominant in a great power competition.

Operationalizing cybersecurity inherently requires close collaboration with the private sector, to include leveraging commercial cybersecurity tools, private capital and technical skillsets from industry; the NSS highlights the criticality of this relationship. A key recommendation from CSC Pillar 5 is to codify the concept of "systematically important critical infrastructure". Achieving this outcome requires a close partnership between the U.S. government and private industry. An emerging technology the United States should deem an important critical infrastructure is 5G wireless networks. Operationalizing cybersecurity in collaboration with the private sector is in part new thinking and approaches to how the U.S. government partners with industry in developing and securing 5G technologies.

This requires U.S. government policies that maximize national security outcomes by pursuing commercially developed technology. The research conducted by the CSC offers two recommendations to achieve this pursuit: 1) codify what infrastructure is deemed critical and systemically important; and 2) establish collaborative environments bringing government and industry together to share threats, information, analysis, and planning. The following discussion explores three policy recommendations that align with this guidance and maximize the benefit of operationalizing cybersecurity with the private sector: 1) pursue a hybrid Joint Capabilities Integration and Development System (JCIDS) and Other Transaction Authority (OTA) 5G wireless Open Radio Access Network (O-RAN) technology; 2) implement fee-simple 5G electromagnetic spectrum (EMS) ownership with non-interference easement; and 3) develop US 5G cybersecurity approaches in coordination with international partners.

6.1 Industry Sectors and Current Conditions

Telecommunication companies (telcos) are the most well-known industry participants in the broad 5G American and global industry sector. Domestically, AT&T and Verizon are the leading telcos in terms of 5G enterprise and consumer technology development and solutions. Beyond mobile carriers, the 5G industry is comprised of network hardware firms manufacturing key components such as: (1) small cell antenna arrays; (2) data converter chips; (3) small chip sets; (4) network processors; (5) field programmable graphic arrays; and (6) small cell power amplifiers. At the moment, American and European firms dominate the global 5G network hardware market; however, Chinese telcos and hardware firms are focused on becoming global leaders in these markets by developing competitive solutions by any means possible.

6.2 Challenges and Outlook

The United States is at a strategic disadvantage regarding the rollout of 5G network infrastructure. A key segment of the network, the Radio Access Network (RAN) segment, currently has no US manufacturers of the hardware required and the United States is already trailing China in 5G RAN development. As a result, China, via Huawei Technologies, has created a strategic advantage in the 5G RAN technology market. Therefore, the United States cannot take any risk or delay in pursuit of an alternative to 5G RAN technology.

Mixing and matching hardware within that network is not possible due to interoperability limitations. A developing alternative technology that addresses China's advantage and interoperability limitations is O-RAN, a technology for the RAN segment of the 5G network. O-RAN will decouple hardware and software solutions from 5G network deployments through vendor-neutral hardware and software-defined technologies based on open interfaces and community-developed standards.

Another challenge to 5G technology development and security entails sub-6 Ghz EMS. There is an ongoing, fierce debate between private industry and DoD over sub-6 Ghz EMS allocation and ownership. The issue centers on a non-market participant, DoD, having exclusive license rights over key EMS required by market participants like U.S. telcos and satellite communications companies.

On one hand, private industry asserts that DoD's ownership of sub-6 Ghz EMS inhibits them from meeting business demand and competing globally against Huawei and ZTE for 5G wireless network coverage. On the other hand, DoD claims industry ownership of exclusive license rights to sub-6 Ghz EMS threatens key U.S. technologies for national security. Instead of debating license ownership under the current EMS allocation system, an alternative approach is feasible. This approach entails redesigning the EMS allocation structure to allow competitive market competition while incorporating non-market interactions. This approach is termed fee-simple ownership with non-interference easement.

Finally, 5G wireless networks require overhauling essential networks, specifically a conversion to software-defined networks. Part of the challenge to this effort involves software maintenance, meaning the expected need to provide routine and emergent software updates, much like the current upgrades to smartphones. Due to the cyber vulnerabilities of software, "the tougher part of the real 5G "race" is to retool how we secure the most important network of the 21st century and the ecosystem of devices and applications that sprout from that network."[2] Never before have the essential networks and services that define lives, economy, and national security had so many participants, each reliant on software and hardware security. Part of this challenge is that none of these participants have the final responsibility for cybersecurity.

It is important to recognize that the 5G dilemma also includes concerns related to data privacy and intellectual property theft. China's lead in deploying 5G networks globally provides unprecedented access that can easily translate to a dominant global intelligence force that facilitates China's progress toward cyberspace superiority.

6.3 Policy Recommendations

Recommendation 6.3.1 Hybrid JCIDS-OTA 5G O-RAN Technology

This recommendation addresses the 5G RAN hardware challenge. A hybrid JCIDS-OTA 5G O-RAN approach pursues JCIDS to validate a joint requirement for O-RAN technology followed by a request for proposals for industry solutions. This process would also include funding authorizations and appropriations for the validated joint requirement. Meanwhile, the Defense Innovation Unit (DIU) would execute a prototype OTA contract through their commercial solutions offering to accelerate prototyping of existing 5G O-RAN solutions. The skills and capabilities to facilitate this OTA is a hallmark of DIU.

The main advantages of this recommendation are risk reduction and validated requirements. The prototyping effort by DIU reduces the timeline for capability development while the JCIDS process validates a joint requirement if no existing technology is identified. A JCIDS-validated requirement with funding will give O-RAN development prioritization and support. However, the disadvantage to this approach is cost. Pursuing both a JCIDS technology development program and DIU prototype will most likely be more expensive than pursuing either alone. Regardless, utilizing a hybrid approach that reduces risk with the JCIDS process, but takes risk with funding existing technology development efforts increases the likelihood that the United States will regain the strategic advantage in wireless networks.

Recommendation 6.3.2 5G EMS Allocation and Management

This recommendation addresses the 5G EMS allocation and management challenge. This approach implements a property-rights EMS allocation and management regime based on market pricing guiding the allocation and exchange of EMS. As a result, public or private sector organizations could purchase and own EMS instead of licensing it with non-interfering easement conditions. This option suggests the U.S. government quickly allow a competitive market for all EMS, including sub-6 Ghz EMS. In the fee-simple ownership with non-interference easement regime, individuals, corporations, and government agencies would be able to buy, sell, and lease specific frequencies in specific locations subject to power/technical limitations. They would also possess the right to emit at any time without interference and could further exchange EMS in secondary markets.

This option has many advantages in terms of efficiency, speed, value, and innovation. From a broad perspective, the United States supports a private-sector-led 5G effort, rather than a government-led nationalized 5G plan. This approach precisely aligns with the U.S. intent to address the current EMS scheme's current failure--chronic inefficient use of valuable EMS. By auctioning all EMS and establishing secondary markets, the pricing mechanism ensures EMS goes to any organization incentivized to maximize the value of the EMS.

In terms of value, an auction where DoD is forced to bid for EMS illuminates the opportunity cost in terms of price of DoD's ownership of EMS and its net present value. That opportunity cost is the market price by which DoD, as an EMS owner and supplier, could exchange sub-6 Ghz EMS with providers in a subsequent secondary market. In addition, this solution facilitates innovation associated with unlicensed EMS that would incentivize incumbents and entrepreneurs to develop new technologies that take advantage of the unlicensed EMS.

Despite the advantages, there is a one perceived disadvantage. Having every federal agency compete for EMS previously granted without competition could result in private industry purchasing EMS critical to national security. This perception is based on incomplete and imperfect EMS market analysis. During the one-year transition period referenced below, federal agencies can conduct independent or collaborative market analysis to estimate the auction cost for purchasing their desired EMS. From that estimation, federal agencies could prioritize their existing annual appropriations to ensure they have the funds to bid and purchase the EMS. For DoD, there have been no EMS auctions that exceeded annual budgets. More importantly, the FCC could transfer the funds agencies used to purchase EMS into their respective accounts at the Treasury Department.

In order to support national objectives at the speed of competitive markets, approval should bypass the standard U.S. interagency policy planning process. Efficient implementation requires that the Federal Communications Commission (FCC) quickly execute this recommendation according to the following broad guidelines:

1) a one-year transition period between U.S. approval and the FCC-led all-EMS auction to allow all market participants, including government agencies, to prepare, and

2) no additional resources of any kind will be allocated to agencies, particularly to DoD, during the transition period; this will motivate DoD to optimize existing resources like a private sector participant in an expectedly competitive market.

Recommendation 6.3.3 Develop 5G Cybersecurity Approaches with Domestic/International Partners

This recommendation addresses the 5G cybersecurity challenge. This approach pursues a U.S.-led international 5G coalition focused on developing interoperable 5G cybersecurity solutions with key allies and partners. While the United States recognizes the risk of worldwide deployment of Huawei 5G, it is also necessary to recognize that this problem cannot be mitigated by the United States alone. There must be cooperation with international partners in order to achieve the desired goals.[74]

Reducing the Chinese lead in 5G requires the United States and its allies to develop meaningful alliances and strategic partnerships that will play a vital role in 21st-century surge and mobilization efforts. As previously discussed, the United States must establish strategic partnerships within the domestic RAN industry, providing federal loans and tax incentives that will enable the US partners to close the gap in the 5G RAN market. Internationally, the United States should establish a 5G alliance that will develop guidance to produce a cost-competitive 5G global infrastructure alternative to Huawei.

The responsibility to successfully implement this guidance requires efforts from both industry and government, domestically and internationally. "The time to address these issues is now before we become dependent on less secure 5G services with no plan for how we sustain cyber readiness for the larger 5G ecosystem."[75] Implementation of the recommendations within this discussion will provide solutions to address market challenges, risk factors, and shortfalls associated with the current state.

Section 7: Conclusion

The Cyber Domain and Advanced Computing Industry study team conducted a broad level of engagements with government agencies, academic institutions, and industry firms leading innovation in the cyberspace ecosystem. This industry has led the expansion of the global economy, and is now the primary competitive domain between the United States, China, Russia, Iran, and North Korea, and violent extremist organizations. Some of these actors support criminal organizations that also conduct cyber operations, allowing the actor to deny culpability.

As the study team members conducted their research, they understood that the United States' technological and economic leadership in this domain is no longer guaranteed to continue for decades, as China aggressively pursues its "China 2025" plan to replace the United States as the leader in ten critical fields by 2025.

At the completion of their research, they had a better understanding of the unique roles that industry, academia, and government agencies play in the innovation and economic health of this ecosystem and the nation. As they considered policy recommendations to address the challenges in this domain, they found significant correlation with many of the findings of the Cyber Solarium Commission Report published in March 2020.

While the 19 recommendations in this paper (outlined in Sections 3-6 and Appendix A) stand on their own merit, the team believes the linkage to the CSC recommendations provides symbiotic support for both reports. It is our hope that senior United States leaders will take action to implement and apply resources to these recommendations. As the members of this study team themselves move to senior positions in the United States, they will be the agents of change to maintain United States leadership in this domain for a peaceful and prosperous world.

Appendix A: National Mobilization Summary

A.1 Domestic Cyberspace Mobilization

Cyberspace "is the domain within the information environment that consists of the interdependent network of IT infrastructures and resident data. It includes the internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations is the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[76] This domain has unique challenges for the U.S. government trying to prepare for mobilization across the industry and firms that work in this space.

The word *mobilization* was first used in a military context in the 1850s to describe the preparation of the Imperial Russian Army. It was coupled with the introduction of conscription and the railways in the 19th century. Its theories and tactics have continuously changed since then, however the concept remains focused around the assembling of armed forces, military reserves, or civilian persons of military age into readiness for active service and organizing or adapting industries, transportation facilities, factories, etc. for service to the government in time of war. Born out of the 1850s, mobilization has traditionally centered around a kinetic war.

Kinetic war largely entailed ensuring raw materials and labor were available for industry to rapidly scale-up *productive capabilities* of national security-relevant items of interest (i.e. tanks, planes, armaments) within a given period of time (i.e. 30 days, 90 days, 1 year), or quickly assembling civilians with general skill sets for service, as the government was capable of bringing personnel to proficiency skill levels in short periods of time. The cyberspace domain across both public and private networks in the United States is characterized by its massive existing capacity, including both personnel and hardware, or data centers. The current COVID-19 crisis has shown how various cyberspace networks in the United States have adapted relatively easily to a significant surge in use by tens of millions of users, in a short window of several weeks. This domain's underutilized operating capacity allows for a more rapid surge capability than is typical in more typical kinetic war domains.

In many ways, the corresponding *mobilization laws, executive orders, regulations, and rules* focus around preparing for kinetic war. This includes the U.S. government's ability to use the Selective Service system for conscription of troops, and other legislation and Presidential authorities to organize industries, including the Defense Production Act (DPA), Executive Order 13806 (EO 13806 Title 3 "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, and Executive Order 13603 (EO 13603) "National Defense Resources Preparedness." However, the 21st century cyberspace environment has drawn the United States into a persistent war that is not kinetic. Mobilization for cyber and advanced computing takes on a different dimension and brings a richer problem set to bear. Although the 1950s era DPA imagined kinetic war, it can still be utilized in the cyberspace domain using the proper sections to address modern challenges.

One of the ways the *current COVID-19 pandemic shows us how the cyberspace domain can be rapidly activated* in order to reduce disease transmission among individuals – is implementation of contact tracing at scale. In the recent pandemic, South Korea successfully decentralized contact tracing authority to the district/local levels by using smart and cost-effective SMS text-based notifications to district/local citizens. South Korean contact tracing also anonymized individuals' data, thus minimizing citizen concerns with privacy violations.[77] Recent collaboration on the development of a robust and shared contact tracing app by Google and Apple that will be functional by the end of May 2020, shows that even bitter U.S. industry rivals can come together in an emergency. Some commentators have noted that U.S. legislative changes may be required in order to allow for involuntary publication of the contact tracing data of individuals infected by COVID, but in a true national health emergency, the

Constitution and existing legal authorities allow both the federal and state governments to take extraordinary actions – including involuntary quarantines – to maintain the public health.[78]

The DPA can still be used to address 21st century cyberspace mobilization problems. In particular, Section 107 can be used to *enhance supply chain security* in the cyberspace domain,[79] focusing on critical technology computer components required to assemble the multiple computing devices comprising today's ubiquitous networks. The most critical of these components are integrated circuit boards and advanced semiconductor chips. China produces nearly 50 percent of global supply of cheaper less complex printed circuit boards required in many electronic devices,[80] and they have made limited progress in manufacturing more advanced semiconductors. Over 70 percent of the world's advanced semiconductors are produced in Asia, principally Taiwan, South Korea, Japan, Singapore, and China. Despite trying to increase market share in this market for 20 years, China's global market share has remained stagnant at around 10 percent, as the complexity of both fab and fabless production has kept it from scaling. While Taiwan has the largest portion of the production market at well over 25 percent, 16 percent remains in the United States, and 10 percent in Europe.[81]

While friendly with the United States and an important production partner of leading American advanced semiconductor designers, Taiwan's dominance of the advanced microchip production market is a potential *supply chain bottleneck.* Given its proximity to China and difficult historical and ongoing tensions with the mainland, the United States should take immediate steps to avoid making this bottleneck worse. The United States could mitigate supply chain security risk by offering greater tax incentives to support domestic firms' production of national chip foundries such as Intel, NVIDIA, and Advanced Micro Devices, and also by offering similar incentives to Taiwanese producers such as Taiwan Semiconductor Manufacturing Company (TSMC) to open up production factories in North America, also increasing domestic production. This could be led by a federal government initiative partnering with interested state governments and industry associations that would be amenable to both tax breaks and other academic and trade industry initiatives to train technical workers. TSMC would be following venerable manufacturing firms from allied nations, such as Toyota, Honda, Mazda, Nissan, and BMW, who have setup significant automobile production facilities to serve the U.S. market, frequently incentivized by low-tax, labor-friendly environments in states such South Carolina, Tennessee, Ohio, Alabama, and Kentucky. The U.S. government should work with states to incentivize both domestic and overseas firms to re-shore semiconductor production capacity in the United States, and if done right, these incentives can generate jobs and industry growth, thereby offsetting potential taxation losses.

Accordingly, cyberspace mobilization has some *supply chain vulnerabilities* as listed above. However, as we have seen with the current pandemic, surging in this domain is not only about simply producing more "widgets" off an assembly line bounded by 'traditional' supply chain bottlenecks, supply chain security, or international supply chain agreements. Instead, cyber mobilization brings the challenge of increasing the capacity of highly specialized equipment and highly skilled personnel in an extremely short duration of time. Existing laws in support of mobilization have largely overlooked this challenge, but can be adapted for use now.

Additional capacity for cyber mobilization exists with our allies. Both the United States and allied nations have considerable manpower and high-performance computing resources, such as millions of additional civilian government and private sector computer engineers and technicians, and significant HPC data centers. Our recommendations detail sectors of the U.S. and other economies that could be diverted towards achieving national security objectives, with the right preparation and incentives. Existing laws must be applied in new ways to develop policies that will harness the nation's limited cyber and advanced computing resources that may not necessarily be scaled rapidly. While this paper limits the discussion to NATO, similar steps can and should be taken with all our partners and allies in the Asian Pacific, Western Hemisphere, and the Middle East.

A.2 International Partners & Cyberspace Mobilization

NATO declared cyberspace as a domain of operations and cyber defense is recognized as part of NATO's core task of collective defense. In 2016, NATO members agreed to a Cyber Defense Pledge to ensure the Alliance keeps pace with the fast-evolving cyber threat landscape and that member nations will be capable of defending themselves in cyberspace as in the air, on land and at sea. Member nations declared their commitment will ensure strong and resilient cyber defenses that will enable the Alliance to fulfil its core tasks.[82] However, the pledge's promises are overly broad and ambiguous. While each ally is responsible for its own cyber defense, NATO pledges to support its members in boosting their defenses by taking the following steps:[83]

- Sharing real-time information about threats through a dedicated malware information sharing platform, as well as exchanging best practices on handling cyber threats;
- Maintaining rapid-reaction cyber defense teams that can be sent to help Allies in addressing cyber challenges;
- Developing targets for Allies to facilitate a common approach to their cyber defense capabilities;
- Investing in education, training and exercises, such as Cyber Coalition, one of the largest cyber defense exercises in the world.

Despite these important steps, NATO is not currently equipped to face cyber threats. The alliance does not have offensive cyber capabilities; its cyber deterrence relies on member nations' deterrence capabilities. Members use their cyber capabilities on behalf of the alliance. Nevertheless, without a well-defined policy agreement and a clear command structure in overseeing NATO operations, this approach is unlikely to work well. In NATO, decisions are agreed upon on the basis common accord and consultations take time. Unfortunately, cyber threats evolve fast and inflict damage in a very short time. To respond to cyber threats in a meaningful manner NATO needs to streamline its decision-making process in the cyber domain, and define potential response scenarios – including and short of -- evoking the collective-defense clause under Article 5. *NATO should further formalize its cyber strategy through top-down guidance and increase its cooperation with partners to broaden their spectrum of potential responses*.[84]

Even if the member nations allocate more cyber offensive capabilities to NATO, integration and command and control, and use of this force pose significant challenges. NATO definition of a cyber-attack, "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects,"[85] leaves significant room for interpretation. As a result, information sharing among allies and partners is critical for situational awareness and preparedness. Twenty-nine NATO allies have different threat perceptions. Information sharing is critical to create a baseline understanding of cyber-threats the alliance faces.

NATO should consider the following steps to increase cyber resilience;[86]

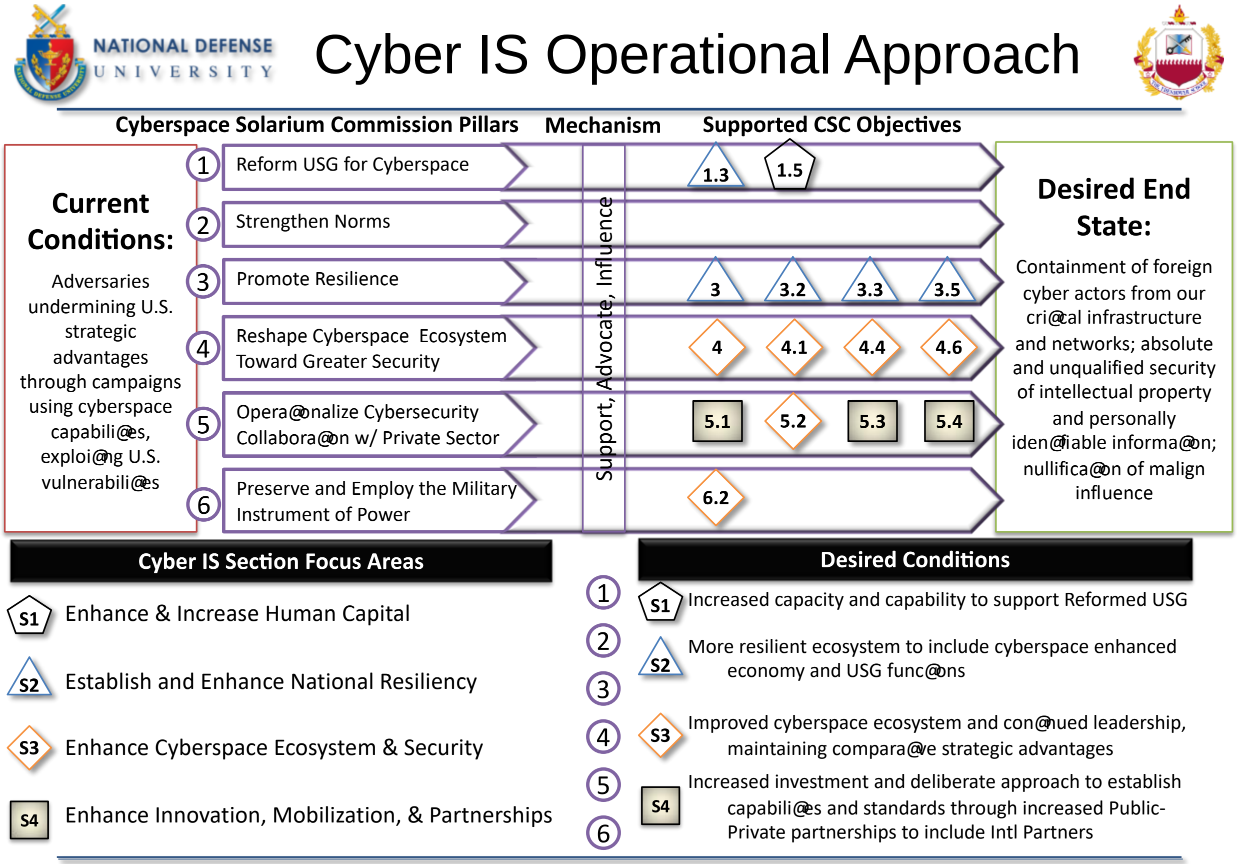
- Formalize strategy through top-down guidance
- Work with partners and expand the spectrum of responses
- Streamline cyber decision-making processes
- Define cyber deterrence and response scenarios

These are not costly innovations requiring significant investment, and this is not simply a recommendation for NATO to follow the largest members' policies and direction. Cyber security investment is a high-value component of NATO member contributions towards reaching a two percent GDP defense spend ratio to their overall GDP. Smaller, newer NATO members such as Estonia have an excellent cyber security strategy, and can add real value to the NATO collective by driving changes in both the strategic and long-term plans for recruiting cyber talent from their citizenry. Estonia's longrunning battle with Russia in cyber space has led to the development of a small but extremely cyber-capable NATO member.[87]

a) As a first step to improve NATO cyber resilience, members need to improve information sharing. We recommend extensive information sharing through Cyber Information Sharing Partnerships, which will constitute a key instrument to face the multiple challenges in cyber domain. Cyber Information Sharing Partnerships will not only enable force multiplication, but it will also increase legitimacy, transparency and credibility of NATO cyber operations.

b) We also recommend that NATO create a Cyber Situational Awareness and Information Exchange (CSA/IE) Forum. The NATO Joint Warfare Center (JWC), NATO Communications and Information Agency (NCI Agency), and the NATO Communication and Information Systems Group (NCISG) can co-facilitate the information exchange. The CSA/IE forum will provide a venue for NATO cyber community to surface and resolve issues that arise among organizations participating in cybersecurity information sharing and implementation of cybersecurity information sharing capabilities, with a focus on sharing speed and integrated operational engagements. The CSA/IE forum will identify cybersecurity information sharing requirements for capability providers, build consensus, share best practices, coordinate and collaborate on activities that enable sharing of cyber threat information to include (but not limited to) indicators, defensive measures, and cyber threat intelligence, while providing NATO allies and partners with the ability to address the range of cyber threats.

Appendix B: Operational Approach Diagram



Cyber IS Operational Approach

NATIONAL DEFENSE UNIVERSITY

Cyberspace Solarium Commission Pillars | Mechanism | Supported CSC Objectives

Current Conditions:

Adversaries undermining U.S. strategic advantages through campaigns using cyberspace capabilities, exploiting U.S. vulnerabilities

1 Reform USG for Cyberspace — 1.3, 1.5

2 Strengthen Norms

3 Promote Resilience — 3, 3.2, 3.3, 3.5

4 Reshape Cyberspace Ecosystem Toward Greater Security — 4, 4.1, 4.4, 4.6

5 Operationalize Cybersecurity Collaboration w/ Private Sector — 5.1, 5.2, 5.3, 5.4

6 Preserve and Employ the Military Instrument of Power — 6.2

Support, Advocate, Influence

Desired End State:

Containment of foreign cyber actors from our critical infrastructure and networks; absolute and unqualified security of intellectual property and personally identifiable information; nullification of malign influence

Cyber IS Section Focus Areas

S1 Enhance & Increase Human Capital

S2 Establish and Enhance National Resiliency

S3 Enhance Cyberspace Ecosystem & Security

S4 Enhance Innovation, Mobilization, & Partnerships

1 2 3 4 5 6

Desired Conditions

S1 Increased capacity and capability to support Reformed USG

S2 More resilient ecosystem to include cyberspace enhanced economy and USG functions

S3 Improved cyberspace ecosystem and continued leadership, maintaining comparative strategic advantages

S4 Increased investment and deliberate approach to establish capabilities and standards through increased Public-Private partnerships to include Intl Partners

Cyberspace Solarium Commission Recommendations: Reform Government, Deny Adversay Benefits, Impose Costs (**Cyber Domain and Advanced Computing Industry Study supported recommendations**)

Pillar	**Key Recommendation**	Enabling Recommendation
1 Reform USG Structure & Organization for Cybersecurity	1.1 Issue and Updated National Cyber Strategy	1.1.1 Develop a Multitiered Signaling Strategy 1.1.2 Promulgate a New Declaratory Policy
	1.2 Create House Permanent Select and Senate Select Committees on Cybersecurity	1.2.1 Reestablish the Ofice of Technology Assessment
	1.3 Establish a National Cyber Director	
	1.4 Strengthen the Cybersecurity and Infrastrures Security Agency	1.4.1 Codiffy and Strengthen the Cyber Threat intelligence Integration Center 1.4.2 Strengthen the FBI's Cyber Mission and the National Cyber Investigative Joint Task Force
	1.5 Diversity and Strengthen the Federal Cyberspace Workforce	1.5.1 Improve Cyber-Oriented Education

Pillar	**Key Recommendation**	Enabling Recommendation
2 Strengthen Norms and Non-Mil Tools	2.1: Create a Cyber Bureau and Assistant Secretary at the U.S. Department of State	2.1.1: Strengthen Norms of Responsible State Behavior in Cyberspace
		2.1.2: Engage Actively and Effectively in Forums Setting International Information and Communications Technology Standards
		2.1.3: Improve Cyber Capacity Building and Consolidate the Funding of Cyber Foreign Assistance
		2.1.4: Improve International Tools for Law Enforcement Activities in Cyberspace
		2.1.5: Leverage Sanctions and Trade Enforcement Actions
		2.1.6: Improve Attribution Analysis and the Attribution-Decision Rubric
		2.1.7: Reinvigorate Efforts to Develop Cyber Confidence-Building Measures
3 Promote National Resilience	3.1: Codify Sector-specific Agencies into Law as "Sector Risk Management Agencies" and Strengthen Their Ability to Manage Critical Infrastructure Risk	3.1.1: Establish a Five-Year National Risk Management Cycle Culminating in a Critical Infrastructure Resilience Strategy
		3.1.2: Establish a National Cybersecurity Assistance Fund to Ensure Consistent and Timely Funding for Initiatives That Underpin National Resilience
	3.2: Develop and Maintain Continuity of the Economy Planning	
	3.3: Codify a "Cyber State of Distress" Tied to a "Cyber Response and Recovery Fund"	3.3.1: Designate Responsibilities for Cybersecurity Services under the Defense Production Act
		3.3.2: Clarify Liability for Federally Directed Mitigation, Response, and Recovery Efforts
		3.3.3: Improve and Expand Planning Capacity and Readiness for Cyber Incident Response and Recovery Efforts
		3.3.4: Expand Coordinated Cyber Exercises, Gaming, and Simulation Enabling Recommendation
		3.3.5: Establish a Biennial National Cyber Tabletop Exercise
		3.3.6: Clarify the Cyber Capabilities and Strengthen the Interoperability of the National Guard
	3.4: Improve the Structure and Enhance Funding of the Election Assistance Commission	3.4.1: Modernize Campaign Regulations to Promote Cybersecurity
	3.5: Build Societal Resilience to Foreign Malign Cyber-Enabled Information Operations	3.5.1: Reform Online Political Advertising to Defend against Foreign Influence in Elections

Pillar	**Key Recommendation**	Enabling Recommendation
4 Reshape the Cyber Ecosystem	4.1: Establish and Fund a National Cybersecurity Certification and Labeling Authority	4.1.1: Create or Designate Critical Technology Security Centers
		4.1.2: Expand and Support the National Institute of Standards and Technology Security Work
	4.2: Establish Liability for Final Goods Assemblers	4.2.1: Incentivize Timely Patch Implementation
	4.3: Establish a Bureau of Cyber Statistics	
	4.4: Resource a Federally Funded Research and Development Center to Develop Cybersecurity Insurance Certifications	4.4.1: Establish a Public-Private Partnership on Modeling Cyber Risk
		4.4.2: Explore the Need for a Government Reinsurance Program to Cover Catastrophic Cyber Events
		4.4.3: Incentivize Information Technology Security through Federal Acquisition Regulations and Federal Information Security Management Act Authorities
		4.4.4: Amend the Sarbanes-Oxley Act to Include Cybersecurity
	4.5: Develop a Cloud Security Certification	4.5.1: Incentivize the Uptake of Secure Cloud Services for Small and Medium-Sized Businesses and State, Local, Tribal, and Territorial Governments
		4.5.2: Develop a Strategy to Secure Foundational Internet Protocols and Email
		4.5.3: Strengthen the U.S. Government's Ability to Take Down Botnets
	4.6: Develop and Implement an Information and Communications Technology Industrial Base Strategy	4.6.1: Increase Support to Supply Chain Risk Management Efforts
		4.6.2: Commit Significant and Consistent Funding toward Research and Development in Emerging Technologies
		4.6.3: Strengthen the Capacity of the Committee on Foreign Investment in the United States
		4.6.4: Invest in the National Cyber Moonshot Initiative
	4.7: Pass a National Data Security and Privacy Protection Law	4.7.1: Pass a National Breach Notification Law
5 Operationalize Cybersecurity Collaboration with the Private Sector	5.1: Codify the Concept of "Systemically Important Critical Infrastructure"	5.1.1: Review and Update Intelligence Authorities to Increase Intelligence Support to the Broader Private Sector
		5.1.2: Strengthen and Codify Processes for Identifying Broader Private-Sector Cybersecurity Intelligence Needs and Priorities

Pillar	Key Recommendation	Enabling Recommendation
		5.1.3: Empower Departments and Agencies to Serve Administrative Subpoenas in Support of Threat and Asset Response Activities
	5.2: Establish and Fund a Joint Collaborative Environment for Sharing and Fusing Threat Information	5.2.1: Expand and Standardize Voluntary Threat Detection Programs
		5.2.2: Pass a National Cyber Incident Reporting Law
		5.2.3: Amend the Pen Register Trap and Trace Statute to Enable Better Identification of Malicious Actors
	5.3: Strengthen an Integrated Cyber Center within CISA and Promote the Integration of Federal Cyber Centers	
	5.4: Establish a Joint Cyber Planning Cell under the Cybersecurity and Infrastructure Security Agency	5.4.1: Institutionalize Department of Defense Participation in Public-Private Cybersecurity Initiatives
		5.4.2: Expand Cyber Defense Collaboration with Information and Communications Technology Enablers
6 Preserve and Employ Military Instrument of National Power	6.1: Direct the Department of Defense to Conduct a Force Structure Assessment of the Cyber Mission Force	6.1.1: Direct the Department of Defense to Create a Major Force Program Funding Category for U.S. Cyber Command
		6.1.2: Expand Current Malware Inoculation Initiatives
		6.1.3: Review the Delegation of Authorities for Cyber Operations
		6.1.4: Reassess and Amend Standing Rules of Engagement and Standing Rules for Use of Force for U.S. Forces
		6.1.5: Cooperate with Allies and Partners to Defend Forward
		6.1.6: Require the Department of Defense to Define Reporting Metrics
		6.1.7: Assess the Establishment of a Military Cyber Reserve
		6.1.8: Establish Title 10 Professors in Cyber Security and Information Operations
	6.2: Conduct a Cybersecurity Vulnerability Assessment of All Segments of the NC3 and NLCC Systems and Continually Assess Weapon Systems' Cyber Vulnerabilities	6.2.1: Require Defense Industrial Base Participation in a Threat Intelligence Sharing Program
		6.2.2: Require Threat Hunting on Defense Industrial Base Networks
		6.2.3: Designate a Threat-Hunting Capability across the Department of Defense Information Network
		6.2.4: Assess and Address the Risk to National Security Systems Posed by Quantum Computing

Appendix C: Adaptive Funding Framework Draft Statutory Language

C.1. Cyber/IT Appropriation (CITA) DRAFT Statutory Language

2022 DOD APPROPRIATIONS ACT, SEC. _____ Cyber/Information Technology Appropriation (CITA).

CYBER AND INFORMATION TECHNOLOGY, [*AGENCY]

For the acquisition, procurement, research, development, testing, evaluation, establishment, expansion, modernization, maintenance, and sustainment of [*AGENCY] information technology and information systems, as defined in as defined in section 11101 of title 40, and DoD national security systems, as defined in section 11103 of title 40, as an IT product or IT service, and other expenses necessary for the foregoing purposes, $XX,XXX,XXX,000, to remain available until September 30, 2025.

C. 2. RDT&E-Other (RDT&E-O) DRAFT Statutory Language

2022 DOD APPROPRIATIONS ACT, SEC. _____ RDT&E-Other (RDT&E-O)

OTHER RESEARCH, DEVELOPMENT, TEST, AND EVALUATION, [*AGENCY]

For expenses necessary for basic and applied scientific research, development, test and evaluation, including maintenance, rehabilitation, lease, and operation of facilities and equipment, which are not otherwise provided as specific pre-programmed budgeted efforts in the RESEARCH, DEVELOPMENT, TEST AND EVALUATION, [*AGENCY], $XX,XXX,XXX,000 to remain available for obligation until September 30, 2024.

C.3. Expense/Investment/RDT&E Threshold (E/I/R-T) Exception DRAFT Statutory Language

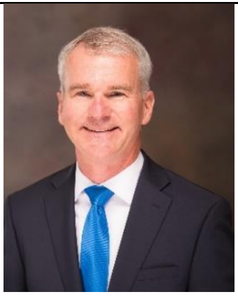
2022 DOD APPROPRIATIONS ACT, SEC. _____ Expense/Investment/RDT&E Threshold (E/I/R-T) Exception

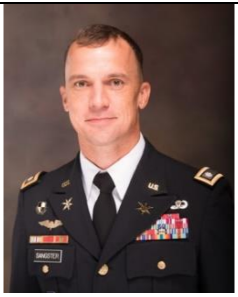
Funds made available in this title to the Department of Defense for operation and maintenance may be used to purchase items having an investment unit cost of not more than $250,000, and for any Research, Development, Test and Evaluation effort having a total cost of not more than $250,000: Provided, That, upon determination by the Secretary of Defense that such action is necessary to meet the operational requirements of a Commander of a Combatant Command engaged in contingency operations overseas, such funds may be used to purchase items having an investment item unit cost of not more than $500,000, and to perform any Research, Development, Test and Evaluation effort having a total cost of not more than $500,000.**

*AGENCY is Defense, Army, Navy/Marine Corps, Air Force, Space Force, and their Reserve or National Guard components, as appropriate

** Underlined portion adds RDT&E efforts to the current Investment-Expense Authority

Appendix D: Industry Study Seminar Members

Dwight D. Eisenhower School for National Security and Resource Strategy Cyber Domain/Advanced Computing Industry Study Academic Year 2019-2020		**Student Lead** **Ms. Stephanie C. Arnold, DOS Management Counselor, U.S. Embassy, Abidjan, Côte d'Ivoire**
 COL Mohammed S. Al Barazanchi, Iraqi Army, MOP Director of Organizing & Planning	 **COL Jose A. Cora, JACG, USA Staff Judge Advocate (SJA), Army Futures Command (AFC)**	 **COL George I. Corbari, USA G5, Army Cyber Command, Chief of Policy, Strategy, and Plans**
 Mr. Jeffrey A. Donnell, DIA United States Central Command (USCENTCOM)	 **Lt Col Jason M. Holcomb, USAF Air Force Material Command, Chief of Financial Analysis**	 **Lt Col Christopher T. Johnson, USAF Space and Missile Systems Center Enterprise Corps, U.S. Space Force**
 **Mr. Daniel O. Joyce, USA Army Program Executive Office (PEO) Enterprise Information Systems (EIS)**	 **Mr. Sahan B. Kamara, DoD Defense Information Systems Agency (DISA)**	 **COL Aydin Kilic, Turkish Army Turkish Armed Forces General Staff, Ankara, Turkey**

 Col Amir Lazar, Israeli Air Force (IAF) Head of Training, Education and Strategic Plans Division	 **CDR Mark A. Lindsey, JAGC, USN United States Transportation Command (USTRANSCOM)**	 **Mr. Andrew D. McClearn, DOS Management Counselor, U.S. Embassy, Santiago, Chile**
 Col Vladimir Milovanovic Republic of Serbia Military Intelligence Agency (MIA) Deputy Head of the Situation Center	 **LTC Benjamin F. Sangster, USA 780th Cyber Brigade, Ft. Meade**	 **Mr. Antonio "T" Scurlock, DHS Cybersecurity and Infrastructure Security Agency (CISA)**
 Colonel Brent O. Skinner, USA Commander, Defense Information Systems Agency-Europe	 **LTC Lance M. Sneed, USA Commander, 266th Financial Management Brigade**	 **Lt Col Randolph B. Witt, USAF Air Staff, A2/6 Directorate - Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations**

Appendix E: Industry Analysis Firm Briefings: IBM, Microsoft, Northrop Grumman, and Verizon

NOTES

[1] "Speech by Franklin D. Roosevelt, New York (Transcript)," online text, Library of Congress, Washington, D.C. 20540 USA, accessed January 13, 2020, https://www.loc.gov/resource/afc1986022.afc1986022_ms2201/?st=text.

[2] History com Editors, "Pearl Harbor," HISTORY, accessed May 4, 2020, https://www.history.com/topics/world-war-ii/pearl-harbor.

[3] Aaron Katersky, "The 9/11 Toll Still Grows: More than 16,000 Ground Zero Responders Who Got Sick Found Eligible for Awards - ABC News," ABC News, last modified 2018, accessed May 14, 2020, https://abcnews.go.com/US/911-toll-growsl-16000-ground-responders-sick-found/story?id=57669657.

[4] Ecosystem | Definition of Ecosystem at Dictionary.Com," https://www.dictionary.com/browse/ecosystem?s= (accessed May 10, 2020).

[5] *Cybercrime Magazine* website, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed January 30, 2020).

[6] Andrew Nichols and Ramberto Torruella, "Cyber Domain/Advanced Computing Industry Study: Industry Overview" (National Defense University, Ft. McNair, Washington DC, January 28, 2020).

[7] Bureau of Labor Statistics, News Release - Beureau of Labor Statistics, Statistics (Washington, DC, 2020), https://www.bls.gov/news.release/pdf/empsit.pdf.

[8] Nichols and Torruella, "Industry Overview".

[9] Nichols and Torruella, "Industry Overview"

[10] President Donald J. Trump, National Security Strategy of the United States of America, December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed May 5, 2020).

[11] President Donald J. Trump, National Security Strategy of the United States of America, December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed May 5, 2020).

[12] "Solarium Commission Report Executive Summary," March 2020, U.S. Cyberspace Solarium Commission. https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view (accessed May 5, 2020).

[13] "Solarium Commission Report Executive Summary," March 2020, U.S. Cyberspace Solarium Commission: https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view (accessed May 5, 2020).

[14] Linda Weiss, America Inc.? Innovation and Enterprise in the National Security State, Cornell University Press, 2014. www.jstor.org/stable/10.7591/j.ctt5hh1c9 (accessed May 5, 2020).

[15] C. Freeman, Technology Policy and Economic Performance, cited in Luc Soete, Bart Verspagen, and Bas ter Weel, Handbooks in Economics, Chapter 27, “Systems of Innovation,” 2010.

[16] Phil Budden and Fiona Murray, “MIT Innovation Ecosystems Stakeholder Model Short Course,” *Massachusetts Institute of Technology,* October 10, 2019.

[17] Budden and Murray, “Innovation Short Course.

[18] The White House, President Barrack Obama, STEM for All, February 11, 2016, https://obamawhitehouse.archives.gov/blog/2016/02/11/stem-all (accessed April 17, 2020).

[19] The White House, STEM Education Funding, September 26, 2017, https://www.whitehouse.gov/articles/president-trump-signs-memorandum-stem-educatoin-funding/ (accessed April 17, 2020).

[20] The White House, Bill Announcement, December 25, 2019, accessed April 17, 2020, http://www.whitehouse.gov/briefings-statements/bill-announcement-73/.

[21] Angus Loten, “America’s Got Talent, Just Not Enough in IT,” *Wall Street Journal*, October 15, 2019. https://www.wsj.com/articles/americas-got-talent-just-not-enough-in-it-11571168626?mod=hp_featst_pos1 (accessed March 19, 2020).

[22] Ben Weiner, “Why the U.S. has a STEM shortage and how we fix it (Part 1),” Recruiting Daily, November 6, 2018, accessed April 16, 2020, https://recruitingdaily.com/why-the-u-s-has-a-stem-shortage-and-how-we-fix-it-part-1/ (accessed March 19, 2020).

[23] William Crumpler and James Andrew Lewis, "The Cybersecurity Workforce Gap," Center for Strategic and International Studies (CSIS), January 2019, p. 1. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf (accessed April 16, 2020).

[24] Wilbur Ross and Elaine Duke, “Supporting the Growth and Sustainment of the Nation’s Cybersecurity Workforce: Building the Foundation for a More Secure American Future,” U.S. Department of Commerce and U.S. Department of Homeland Security, May 30, 2018, p. 1-2. https://www.cisa.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf (accessed April 16, 2020).

[25] Crumpler and Lewis, p. 2-3.

[26] Chase Gunter, "Cyber Workforce Order Doesn't Solve the Retention Problem," *FCW*, May 9, 2019. https://fcw.com/articles/2019/05/09/cyber-order-retention-solve-gunter.aspx (accessed April 16, 2020).

27. Andy J. Semotiuk, "Recent Changes to the H1B Visa Program and What is Coming in 2019," *Forbes*, January 2, 2019. https://www.forbes.com/sites/andyjsemotiuk/2019/01/02/recent-changes-to-the-h1b-visa-program-and-what-is-coming-in-2019/#456df55e4a81 (accessed March 21, 2020).

28. Deborah D'Souza, "The H-1B Visa Issue Explained," *Investopedia*, June 25, 2019. https://www.investopedia.com/news/h1b-visa-issue-explained-msft-goog/ (accessed March 21, 2020).

29. Jie Zong and Jeanne Batalova, "International Students in the United States," Migration Policy Institute *Spotlight*, May 9, 2018. https://www.migrationpolicy.org/article/international-students-united-states (accessed March 22, 2020).

30. According to a Congressional Research Service study, for the school year 2017-2018, India had 154,000 STEM students studying at US universities, Saudi Arabia had 20,000 STEM students in the US, South Korea had 17,000, Taiwan had 9,000, Kuwait had 7,000, and Canada had 6,000. Both India and Saudi Arabia are key regional partners to the US as it seeks to counterbalance China and Iran. Increasing the number of H-1B visa to students from these countries once they graduate could help in that effort. "Foreign STEM Students in the United States" Congressional Research Service, In Focus, November 1, 2019, 2017, https://crsreports.congress.gov/product/pdf/IF/IF11347 (accessed April 16, 2020).

31. Arthur Herman, "America's STEM Crisis Threatens our National Security," *American Affairs Journal*, Spring 2019, Vol. III, No. 1. https://americanaffairsjournal.org/2019/02/americas-stem-crisis-threatens-our-national-security/ (accessed March 10, 2020).

32. Zong and Batalova.

33. Apprentice Toolbox, "Apprenticeship System in Germany," October 4, 2019. https://www.apprenticeship-toolbox.eu/germany/apprenticeship-system-in-germany/143-apprenticeship-system-in-germany (accessed March 25, 2020).

34. George Seffers, "Calling for a Civilian Cyber Corps," Signal Magazine, May 1, 2019. https://www.afcea.org/content/calling-civilian-cyber-corps (accessed April 16, 2020).

35. Ross and Duke, p. 1.

36. Angus King and Mike Gallagher, "Cyberspace Solarium Commission Report" (Washington, DC: Congress of United States, March 11, 2020), 1, https://www.solarium.gov/report (accessed May 10, 2020).

37. King & Gallagher, p. 54

38. King & Gallagher, p. 54

39. King & Gallagher, p. 54

40. King & Gallagher, p. 54.

41. Tom Wheeler and David Simpson, "Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the most important network of the 21st Century." Brookings Institute, September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/ (accessed April 16, 2020).

42. "National Strategy to Secure 5G" (The White House, March 2020), https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf. (accessed April 16, 2020).

43. World Economic Forum, *The Impact of 5G: Creating New Value across Industries and Society* (Geneva, Switzerland, 2020), http://www3.weforum.org/docs/WEF_The_Impact_of_5G_Report.pdf; Fabian Jansen, "Big Data & Analytics in Industry," *Ieee* IEEE 5G (2013), https://futurenetworks.ieee.org/images/files/pdf/applications/Data-Analytics-in-5G-Applications030518.pdf; Malik Saadi, *5G In Emerging Markets -*, 2019, https://www.developingtelecoms.com/images/reports/5g-em-report-final-1023-4.pdf?isMambot=1. (accessed April 17, 2020).

44. King & Gallagher, p. 4.

45. King & Gallagher, p. 4.

46. King & Gallagher, p. 4.

47. King & Gallagher, p. 90.

48. King & Gallagher, p. 4.

49. Arthur Herman, "America's STEM Crisis Threatens our National Security," *American Affairs*, February 20, 2019. https://americanaffairsjournal.org/2019/02/americas-stem-crisis-threatens-our-national-security/ (accessed March 23, 2020).

50. King & Gallagher, p. 121.

51. "Use Passwordless Authentication to Improve Security," https://www.microsoft.com/en-us/security/business/identity/passwordless (accessed May 3, 2020).

52. Jeremy Hsu, "Is the U.S. Lagging in the Quest for Quantum Computing?" *Scientific American*, December 6, 2018. https://www.scientificamerican.com/article/is-the-u-s-lagging-in-the-quest-for-quantum-computing/ (accessed March 20, 2020).

53. Hsu, "Is the U.S. Lagging...?"

[54] H.R. 2667 – National Quantum Initiative Act, December 21, 2018. https://www.congress.gov/bill/115th-congress/house-bill/6227 (accessed March 24, 2020).

[55] National Security Council Report No. 68, "A Report to the National Security Council by the Executive Secretary on United States Objectives and Programs for National Security," April 14, 1950. https://digitalarchive.wilsoncenter.org/document/116191 (accessed December 8, 2019).

[56] C. Freeman, *Technology Policy and Economic Performance*, cited in Luc Soete, Bart Verspagen, and Baster Weel, *Handbooks in Economics*, Chapter 27, "Systems of Innovation," 2010.

[57] Department of Defense Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," Office of the Under Secretary of Defense for Acquisition and Sustainment, January 23, 2019. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2019-10-25-134150-283 (accessed April 17, 2020).

[58] Pete Modigliani and Su Chang, "Defense Agile Acquisition Guide: Tailoring DOD IT Acquisition Program Structures and Processes to Rapid Deliver Capabilities," *The MITRE Corporation,* March 2014. https://www.acqnotes.com/Attachments/MITRE-Defense-Agile-Acquisition-Guide.pdf (accessed April 17, 2020).

[59] Department of Defense Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," Office of the Under Secretary of Defense for Acquisition and Sustainment, January 23, 2019: 13. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002p.pdf?ver=2019-10-25-134150-283 (accessed April 17, 2020).

[60] Lindsey Sheppard, Robert Karlen, Andrew Hunter, and Leonardo Balieiro, "Artificial Intelligence and National Security," CSIS, November 2018. https://csisprod.s3.amazonaws.com/s3fspublic/publication/181102_AI_interior.pdf?6jofgIIR0rJ2qFc3.TCg8jQ8p.Mpc81X (accessed April 26, 2020).

[61] RAND Study, "The DoD Posture for AI," RAND, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4229/RAND_RR4229.pdf (accessed April 26, 2020).

[62] Peter Suciu, "The digital defense workforce: Is DoD doing its part to hire for skill and potential," Digital Defense, January 22, 2020. https://news.clearancejobs.com/2020/01/22/the-digital-defense-workforce-is-dod-doing-its-part-to-hire-for-skill-and-potential/ (accessed April 14, 2020).

[63] Task Force Members and BPC Staff, "Building a F.A.S.T. Force: A flexible Personnel System for a Modern Military," Bipartisan Policy Center. https://bluestarfam.org/wp-content/uploads/2017/04/BPC-Defense-Building-A-FAST-Force.pdf (accessed April 14, 2020).

[64] *The Covid-19 High Performance Computing Consortium,* The COVID-19 High Performance Computing (HPC) Consortium is a unique private-public effort spearheaded by the White House Office of

Science and Technology Policy, the U.S. Department of Energy and IBM to bring together federal government, industry, and academic leaders who are volunteering free compute time and resources on their world-class machines. https://covid19-hpc-consortium.org/ (accessed May 3, 2020).

65. Scott Rose, Oliver Borchert, Stu Mitchell and Sean Connelly, "Zero Trust Architecture," National Institute of Standards and Technology (NIST), (2020), p.1.

66. Rose et al, "Zero Trust Architecture", pp. 37-38. https://csrc.nist.gov/publications/detail/sp/800-207/draft, (accessed May 19,2020)

67.Mark Camillo, "Cyber Risk and the Changing Role of Insurance," *Journal of Cyber Policy*, 2:1, DOI: 10.1080/23738871.2017.1296878, 2017, p. 53.

68. IBM website, https://www.ibm.com/security/data-breach (accessed January 30, 2020).

69. *Cybercrime Magazine* website, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed January 30, 2020).

70. Anthony Gambardella, "Cyber Liability Insurance in the US," IBISWorld Industry Report, OD4778, *IBISWorld*, July 2019, p. 3.

71. Camillo, p. 54.

72. Camillo, p. 62.

73. Daniel Woods and Andrew Simpson, "Policy Measures and Cyber Insurance: A Framework," Journal of Cyber Policy, 2:2, DOI:10.1080/23738871.2017.1360927, p. 214.

74. Tom Wheeler and David Simpson, "Why 5G requires new approaches to cybersecurity," Brookings, September 3, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/ (accessed May 9, 2020).

75. Wheler and Simpson, "5G Cybersecurity."

76. Overview of Cyberspace and Cyberspace Operations, "Joint Publication 3-12: Cyberspace Operations," June 8, 2018, p. I-1.

77. Jose Cora, "Decentralizing The U.S. Legal and Policy Regimes for Improved Pandemic Responses," *Eisenhower School Research Paper,* May 2020, pp. 6-9.

78. Cora, "Decentralizing Responses," pp. 9-15.

79. The Defense Production Act of 1950 as Amended, Sec. 107. STRENGTHENING DOMESTIC CAPABILITY [50 U.S.C. App. § 2077.

[80] Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, "*Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*," September, 2018, p. 48.

[81] The McKinsey Global Institute, "China and the world: Inside the dynamics of a changing relationship," July 2019, P. 80. https://www.mckinsey.com/featured-insights/china/china-and-the-world-inside-the-dynamics-of-a-changing-relationship, (accessed May 10, 2020).

[82] . NATO, "Cyber Defence Pledge," NATO, http://www.nato.int/cps/en/natohq/official_texts_133177.htm. (accessed May 5, 2020).

[83] NATO, "NATO Cyber Defence Factsheet," February 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf. (accessed May 9, 2020).

[84] Sophie Arts, "Offense as the New Defense: New Life for NATO's Cyber Policy," The German Marshall Fund of the United States, December 13, 2018, http://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy. (accessed April 27, 2020).

[85] Michael J. Norris, "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace," *Inquiries Journal* 5, no. 10 (2013), http://www.inquiriesjournal.com/articles/775/the-law-of-attack-in-cyberspace-considering-the-tallinn-manuals-definition-of-attack-in-the-digital-battlespace. (accessed May 10, 2020).

[86] Arts, "Offense as the New Defense."

[87] Stephanie Arnold, "A National Mobilization to Grow the U.S. Cybersecurity Workforce," *Eisenhower School Research Paper,* May 2020.