Winning in Cyberspace by Improving Coordination, Supporting Innovation, and Securing Supply Chains

AY 2020-2021
Cyberspace and Advanced Computing Industry Study
Final Report

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

Contents

Student and Faculty Acknowledgement

Russell Mattern, OD, Professor, College of Information & Cyberspace
J. Robert Garverick, Instructor, National Defense University-Eisenhower School

Amanda Okeson, Colonel, United States Air Force
Andrew Ra, Commander, United States Navy
Anthony Lang, Lieutenant Colonel, United States Air Force
Heather Fisk, Lieutenant Colonel, United States Army
Heather Goethert, FS-01, United States Department of State
Heather Putman, GS-15, Department of the Army Civilian
Joshua Simpson, Lieutenant Colonel, United States Marine Corps Reserve
Kristen Wood, Lieutenant Colonel, United States Air Force
Laverne Amara, Lieutenant Colonel, United States Army
Mark Pannell, FS-01, United States Department of State
Miroslaw Postolowicz, Colonel, Polish Army
Nyatigo Marwanga, Colonel, Kenya Army
Odin Klug, Captain, United States Navy
Rhea Pritchett, Lieutenant Colonel, United States Army
Roger Perrault, GS-14, United States General Services Administration
Thelma Piper, Lieutenant Colonel, United States Army National Guard

List of Acronyms

5G – fifth generation
IoT – internet of things
R&D – research and development
RDT&E – research, development, test, and evaluation
STEM - science, technology, engineering, and mathematics
SWOT - strengths, weaknesses, opportunities, and threats

Executive Summary

In the 21st century, cyberspace and the advanced computing industry are at the heart of great power competition and the rapidly changing character of war. How well the United States competes in this industry will impact its economic and national security. U.S. cyber policy influences the conduct of the government, business, civil society, and individuals, and it cuts across political, legal, economic, and ethical interests. Because of the impact of cyber policy on all facets of American life and the breadth of policy required, it is essential for the U.S. government to coordinate and orchestrate lines of effort to achieve desired objectives. This paper examines the current cyber strategic environment, surveys significant stakeholders and their interests, analyzes the strengths and weaknesses of key international players, describes the industry's outlook, and makes recommendations for U.S. policy. Key recommendations include restructuring the U.S. government to orchestrate better domestic policy and international leadership, investing in innovation and human capital to remain competitive, and securing and diversifying strategic supply chains.

Strategic Environment

The strategic environment related to cyberspace and the advanced computing industry is one of *increasing competition, complexity, and risk*. In the context of great power competition, near-peer competitors are catching up and threatening to overtake the technological advantage the United States historically enjoyed. Technological competition with rising authoritarian powers threatens the U.S.-backed liberal world order. U.S. economic security is increasingly reliant on global digital connectivity; however, escalating criminal and nation-state-sponsored cyberattacks expose vulnerabilities in U.S. and allied supply chains and critical infrastructure. Little international consensus exists on cyberlaw, technical standards, or norms. The United States lacks a comprehensive, whole-of-nation strategy to manage a rapidly evolving and complex strategic cyberspace environment. Compounding the challenge, the United States faces a critical shortage of human capital with needed technical cyber skills and outdated procurement processes that do not keep pace with rapidly evolving threats.

Stakeholders and Interests

Key stakeholders in cyberspace and the advanced computing industry include a cross-section of government, industry, civil society, and international parties. These stakeholders have conflicting interests in ethics, economic growth, business opportunity, security, equity, privacy, and human rights. Closer communication and collaboration between all stakeholders are essential for meeting challenges in cyberspace and balancing competing interests.

Competitive Landscape

This paper assesses the global competitive landscape by focusing on five influential countries: the United States, China, Russia, India, and Taiwan. Porter's Diamond and Strengths, Weaknesses, Opportunities, and Threats (SWOT) analyses illuminate the U.S. position within the global competitive landscape. China and Russia continue to deploy powerful cyber warfare tools to influence, steal from, and threaten the United States and its allies and partners. At the

same time, the United States is dependent on Chinese-manufactured cyberspace and advanced computing products. China rivals U.S. capabilities in some emerging technologies such as artificial intelligence and machine learning. India's power resides in its software and programming prowess and its untapped, vast domestic market. India is not yet able to challenge China in manufacturing hardware. Taiwan is a critical global supplier of hardware, particularly semiconductor components. Growing tensions between China and Taiwan underscore the risk of concentrating critical supply chains in one country or region.

Industry Outlook

The industry outlook is one of explosive growth and rapid change. Key issues include the global semiconductor chip shortage, the evolution of quantum computing along with its impact on cryptology and cybersecurity, the rapid spread of fifth-generation (5G) telecommunications, the associated integration of technology into almost all aspects of life through the internet of things (IoT), and the widespread adoption of artificial intelligence. Other key trends include intensifying competition for skilled labor and natural resources, such as rare earth metals, and the transition to zero trust security architecture to manage the risk of cyberattack.

Policy Recommendations

To meet the economic and national security challenges posed by global competition in cyberspace and the advanced computing industry, the U.S. government should:

1. Develop and implement national cyberspace and innovation strategies and establish institutions to coordinate and execute the policy.
2. Strengthen and leverage public-private partnerships to improve cybersecurity and global competitiveness in the advanced computing industry.
3. Strengthen and leverage alliances and international partnerships while establishing international norms in cybersecurity and emerging technologies.
4. Develop, attract, and retain human capital from the science, technology, engineering, and mathematics (STEM) fields to improve U.S. competitiveness.
5. Diversify and strengthen strategic technology supply chains.
6. Modernize and streamline acquisition processes to fund emerging technologies required to meet growing cyber threats.

Conclusions

Rapid technological change in cyberspace and the advanced computing industry pose a complex strategic challenge for the United States. The U.S. government is not currently structured or resourced to adequately respond to the challenge. Recommended policies will help the U.S. government coordinate and orchestrate policy efforts, improving U.S. and allied cybersecurity and competitiveness within the great power competition. Enacting these recommendations will bolster U.S. competitiveness by supporting a pipeline of skilled and innovative talent while protecting critical supply chains that undergird the U.S. economy and, indeed, the U.S.-backed liberal world order.

Introduction

To ensure the survival of the western liberal order, the United States must maintain technological competitiveness in cyberspace with its partners and allies. To maintain parity and achieve overmatch, the United States must streamline cyber coordination across the private, public, and international arenas, catalyze innovation to ensure an edge in disruptive technology, and defend U.S. supply chains to protect the economy.

It is nearly impossible to put a boundary around cyberspace and the advanced computing domain. The Department of Defense defines cyberspace as *"a global domain within the information environment consisting of the interdependent network of information technology infrastructure and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."*[1] The Merriam-Webster Dictionary defines a domain *"as a sphere of knowledge, influence, or activity."*[2] Advanced computing is sophisticated computers and the processes and skills used on these computing systems. By definition, cyberspace and the advanced computing industry encompass the physical, logical, and human components that make information technology possible. It touches every aspect of a 21st century way of life: national security in the form of emerging technology and cybersecurity; economic prosperity in digitized and interconnected economies; infrastructure by way of 5G telecommunications and smart cities; and social connections with the prevalence of social media platforms and other means of digital entertainment.

Few things are untouched by cyberspace; as the world continues the transition from the Industrial Age to the Information Age, new challenges arise. The United States has re-entered a period of great power competition. However, unlike great power competitions of the past, today's great power competition is arguably more complex and dynamic due to the impact of modern technology. The interdependence of the global economies, nuclear weapons, and communications at the speed of light has changed the strategic environment to persistent gray-zone conflict. The United States and its partners and allies are now under constant attack via weapons in cyberspace just below the level of active armed conflict.

The threat is undeniable. During the Industry Study research, the United States contended with the Solar Winds supply chain attack, the hacking and attempted sabotage of a water treatment plant in Florida, a significant breach of Microsoft exchange servers, and a ransomware attack that shut down the largest oil pipeline in the nation.[3] Nefarious actors are undermining the global order, resetting the norms of international behavior, and countering U.S. economic advantages. The U.S. government must streamline cyber coordination across the private, public, and international arenas to address these security challenges. Additionally, it needs to catalyze innovation to ensure a technological advantage in disruptive technology and defend U.S. supply chains to protect the economies.

To tackle this diverse challenge, a team of students from the National Defense University Eisenhower School - Cyberspace and Advanced Computing Industry Study (hereafter referred to as the Industry Study) embarked on an aggressive five-month campaign to understand, scope, and address the most pressing U.S. cyber issues. This campaign was no easy task. The Industry Study wrestled with this vast domain through academic research, in-depth discussion of current

events, and 29 virtual engagements with over 70 representatives from the public, private, and academic sectors. While pandemic restrictions were an obvious limitation, they were not debilitating. The ability of the Industry Study to connect with a diverse group of partners is a credit to the state of U.S. digital technology. While the benefits of these digital technologies enabled the Industry Study to continue during the COVID-19 pandemic effectively, it illuminated the ever-increasing risks and challenges of relying on these digital technologies.

The Industry Study worked through diverse topics including, but not limited to:

- The practical application and limitations of quantum computing,
- The threats of disinformation,
- The management of human capital resources,
- The difficulties in maintaining an innovation advantage,
- The technical intricacies of the open systems interconnection stack, and
- The ethical use of artificial intelligence.

For this analysis, the Industry Study separated the problems into three key themes: *cyber coordination*, *innovation*, and *supply chain security*. After analyzing these overarching themes, this paper proposes six recommendations for the federal government, in partnership with the private sector, to ensure the United States remains competitive in the cyberspace and advanced computing domain. The United States must refocus on competing in cyberspace or risk ceding its global community leadership role.

Section 1: Field Study Organizations

The Industry Study explored five segments within the cyberspace domain that have implications on U.S. national security: telecommunications, information technology services, hardware, software, and human capital. This exploration included several leading cyberspace industry partners from the United States, India, and Taiwan. The Industry Study engaged about cybersecurity and national security interests with the Cyber Threat Alliance, Defense Information Systems Agency, Federal Bureau of Investigation, National Security Agency, United States Cyber Command, and the Department of Homelands Security – Cybersecurity and Infrastructure Security Agency. An engagement with Carnegie Mellon University enabled discussion on the need for continued corporate, government, and institutional partnerships for innovation. In addition to emphasizing the importance of continued partnerships for innovation, the Industry Study discussed with Carnegie Mellon University the importance of venture capital investments for accelerator programs and the importance of STEM education to innovation. See Appendix A for a graphic of the industry partners engaged.

The Industry Study gained a better understanding of China's views on cyberspace and intellectual property through engagements with the U.S. Patent and Trademark Office, the American Institute of Taiwan, the Industrial Technology Research Institute, and the National Defense University – Institute of National Strategic Studies.

The telecommunication industry includes a wide range of transmitting technologies and infrastructure used to exchange voice, data, and video transmissions over significant distances.[4] Interviews in the telecommunications segment included Verizon and the Cellular Telecommunications Industry Association. These engagements covered 5G telecommunications infrastructure, encryption technologies, edge computing, industry standards, and market supply chain.

The information technology services industry includes business processes, applications, and infrastructure services. Engagements with Microsoft, Google, and Amazon were essential in analyzing cybersecurity and cloud computing services. An engagement with Facebook included discussing cybersecurity risks on social media platforms, influencing operations, and inauthentic behavior. Research of Industrial Control Systems through the prism of cybersecurity emphasized critical infrastructure and cyber kill chain case studies. Finally, an interview with Costco provided a unique insight into a global corporation's business process, cybersecurity management, infrastructure services, and ethical sourcing of bulk commercial supplies.

The hardware industry includes all physical components essential to computing. Segments of the hardware market include client computing, storage, servers, networking, and security.[5] During the Industry Study's engagements, discussions with NVIDIA, D-Wave, Etron, and Advantech facilitated research in the hardware segment of cyberspace. The primary focus of the hardware segment was the criticality of semiconductors to artificial intelligence, machine learning, cloud computing, robotics, and quantum computing. In addition to advancements in semiconductor technology, the Industry Study researched supply chain security and the global semiconductor shortage.

The software industry includes the subscription and sales of software applications. The primary market segments are business processes, data and analytics, information technology management, and security.[6] Engagements with D-Wave, IBM, and Rigetti enabled discussion on software advancements and professional services for quantum computing. Interviews with Microsoft, IBM, Google, and Palo Alto Networks examined topics such as software engineering, improved use of automation, software-based advanced analytics, and cloud services.

Human capital is the economic value of an employee's education, training, personal values, skills, and experience.[7] The cyberspace workforce includes specialists who build, operate, and maintain systems and networks. Cyberspace is a highly competitive environment with industry, academia, and governments competing globally to acquire, maintain and optimize personnel from a limited pool of qualified information technology professionals.[8] Human capital is a multi-dimensional topic that impacts all segments of the cyberspace domain. The Industry Study discussed STEM education, recruitment, and human capital management with all organizations engaged.

In addition to human capital, other topics discussed with all industry partners, governmental agencies, and academic institutions included cyber threat intelligence sharing, industry standards, governance, partnerships, and supply chain security.

Section 2: Strategic Environment

Since the end of the Cold War, the United States has enjoyed great prosperity, security, and relative peace as the lone global superpower. Today, the cyberspace and advanced computing industry strategic environment is increasingly complex and challenging due to the rise of authoritarian powers seeking to outpace the United States economically, politically, and militarily. China, Russia, Iran, and North Korea consistently undermine the U.S.-backed, liberal world order and threaten U.S. national security. During his first speech to Congress, President Joseph Biden acknowledged this threat when he stated, "the U.S. competes with China and other countries to win the 21st century."[9] Now is the time for the United States to seriously address adversarial nations' malicious activities against the United States in cyberspace. This section of the paper will provide a brief overview of the critical strategic concerns the United States must address to succeed in the 21st century.

Lack of International Cyber Laws, Technical Standards, and Norms

Global cyberspace and the advanced computing industry lack a consistent set of international cyber laws, technical standards, and norms for how countries act and respond to activities and incidents within cyberspace. While there are many disparate international cyber laws and agreements, there is no consensus among nations on an international treaty that codifies rules of engagement for dealing with malicious activity, crime, and espionage in cyberspace. The United States must seek to establish an international cyber treaty that leverages critical aspects from the Budapest Convention on Cybercrime and the Tallinn Manual 2.0-The International Law Applicable to Cyber Operations.[10]

Lack of a Whole-of-Nation Cyber Strategy

The United States lacks a whole-of-nation cyber strategy and policy that leverages all facets of the nation's cyber resources. Moreover, there is distrust between different agencies within the federal government and between the U.S. government and the private sector. In the event of a cyberattack of significant consequence or national emergency, the United States lacks a national coordination mechanism between federal and state governments and amongst public and private organizations to respond adequately. For example, the sharing of real-time cyber threat intelligence between the public and private sectors is a significant challenge. Additionally, public, private, state, and local emergency cyber response teams rarely coordinate and synchronize tactics, techniques, and procedures in national or regional exercises to prepare for the worst-case cyber scenario by a near-peer adversary.

Cyber Threat Actors: China, Russia, Iran, and North Korea

China, Russia, Iran, and North Korea threaten U.S. national security and the American way of life. They gain a competitive advantage over the United States through successful cyberattacks, cyber espionage activities, critical infrastructure disruptions, supply chain infiltration, and disinformation campaigns. The United States must seek to leverage the DIME (Diplomatic, Informational, Military, and Economic) instruments of national power to deter these nations' nefarious cyber activities.

China is a sophisticated adversary that poses an existential threat to the United States through massive cyber espionage operations to advance the Chinese economy and military weaponry by strengthening its technological posture. Moreover, China sponsors over 45 cyber threat and hacker groups, with four affiliated with the People's Liberation Army directly.[11] Between 2000 and 2020, the United States attributed 152 cyber espionage incidents to China. Additionally, U.S. companies have pursued over 1,200 intellectual property theft cases against Chinese entities in either the U.S. or Chinese court systems.[12] Most recently, in March 2021, a Chinese government-sponsored group targeted Microsoft's enterprise email software and attempted to steal data from 30,000 global organizations.[13] These types of incidents will continue to erode the U.S. worldwide posture; the United States and allies must counter with a coordinated and robust response short of armed conflict.

Russia, a more overt and aggressive threat, is another sophisticated adversary with superior cyber capabilities, access, and demonstrated capacity to cause significant damage to the United States. Moreover, Russia weaponizes social media to influence and divide the U.S. citizenry. The Russian government sponsors seven cyber threat and hacker groups, two with the Russian Federation (GRU) affiliation and one with the Russian Foreign Intelligence Service (SVR) affiliation.[14] Russia's revolutionary strategy to use social media to influence the 2016 U.S. presidential election through social media weaponization operations revealed major vulnerabilities in U.S. national security and demonstrated that virality trumps veracity.[15] During the 2016 presidential election campaign season, the Russian state-sponsored Internet Research Agency (IRA) directed the first-ever large-scale social media weaponization operation against the United States. The IRA cleverly used 400 employees as internet trolls to create and manage over 60,000 automated botnet accounts, 3,000 Russian sock puppets (fake personas), and six hacktivist personas across all major U.S. social media platforms (Facebook, Twitter, Instagram, Reddit, LinkedIn, YouTube, and Tumblr).[16] The IRA methodically exposed over 146 million Americans to false and divisive information. In 2020, the United States attributed the SolarWinds software supply chain cyberattack to the Russian Foreign Intelligence Service, which disrupted 16,000-18,000 computer systems worldwide.[17] In May 2021, the United States attributed the ransomware attack on the U.S. firm Colonial Pipeline to the Russian threat group DarkSide.

Iran's government sponsors only 12 cyber threat groups yet still threatens the United States.[18] These groups conducted cyberattacks to influence the 2020 U.S. presidential election, including critical infrastructure attacks and cyber espionage worldwide. For example, during the 2020 U.S. presidential election, the Iranian threat group Phosphorous targeted 241 presidential campaign email accounts.[19] Between April and July 2020, an Iranian threat group conducted multiple cyberattacks against Israeli water infrastructure facilities.[20] The attackers attempted to poison drinking water by increasing the chlorine levels in the water.[21] Lastly, between 2013 and 2017, the threat group Silent Librarian successfully conducted cyber espionage activities against 176 universities across 21 countries, five U.S. government agencies, 36 U.S. private companies, 11 foreign companies, and two international non-governmental organizations.[22] The attack resulted in the transfer of 31.5 terabytes of data, $3.4 billion of intellectual property loss, and compromised 7,998 accounts worldwide and 3,768 U.S.-based university professor accounts.[23]

Iran wields formidable cyber capabilities that could debilitate the U.S. and allies' critical infrastructure if coupled with Russia or China aggression.

North Korea has a growing cyber capability. North Korea demonstrated the capacity to cause limited disruptions to the private sector and business networks through four state-sponsored cyber threats and hacker groups.[24] The two most notable cyberattacks were the Sony Pictures Entertainment attack in December 2014 and the WannaCry Ransomware attack in May 2017. The Lazarus threat group (also known as APT 38) conducted both attacks. The WannaCry Ransomware attack targeted Microsoft Windows operating systems, infecting 230,000 computer systems across 150 countries and causing an estimated $4 billion in losses worldwide. Lazarus has also conducted operations against 16 organizations across 11 countries. North Korean threat actors prefer Ransomware attacks against private sector entities to extort money. A whole-of-nation cyber strategy adequately coordinated between the federal government and the private sector could deter North Korean threat actors' activities.

Vulnerable U.S. Cyberspace Supply Chains and Critical Infrastructure

The U.S. cyberspace and advanced computing industry supply chains and critical infrastructure are increasingly vulnerable to nefarious activities in cyberspace. Supply chains are a challenge because the industry depends on legacy hardware and software components manufactured overseas. For instance, China is notorious for embedding malicious code or placing spyware in U.S. public and private entities' hardware and software products for intelligence, espionage, or intellectual property theft.[25] Moreover, malicious actors consistently probe, attack, or exfiltrate data from the 16 U.S. critical infrastructure sectors, as illustrated in figure 1.

Cyberspace Research and Development (R&D) Investment

U.S. university-based research and development (R&D) investment is declining. A key indicator of innovation in any country is the money spent on R&D as a percentage of gross domestic product. Per the World Bank, the United States spends 2.7% of the gross domestic product on R&D and is ranked ninth globally in the amount invested; 72% comes from the private sector.[26] Most concerning is data highlighting that the United States continues to fall in the global ranking of government funding for university R&D to 28th, spending only 0.20% of U.S. gross domestic product in 2017.[27] The Defense Department allocates only 15.3% of its Research, Development, Test & Evaluation funding to science and technology efforts, which is deemed essential for future military systems' inception and advancement in the environment of great power competition.[28]

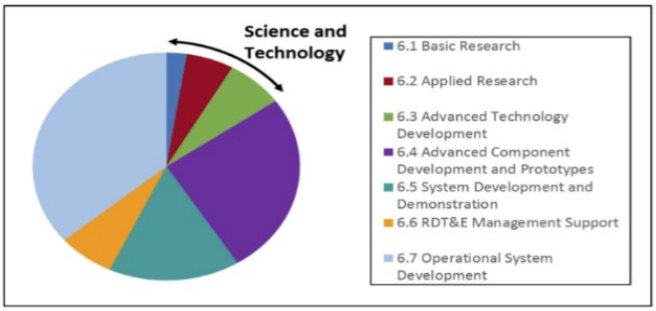

Figure 1. RDT&E budget for science and technology (disruptive innovation) by the Congressional Research Service.

This investment pales in comparison to leading industry partners that exceed 25%. Most cutting-edge technology companies are small businesses with limited capital.[29] Contractors on the bleeding edge of technology must choose between supporting the Department of Defense and seeking lucrative deals from adversarial nations, such as China, that would ensure their survival. Without additional government resources, these small businesses will fail or take their innovative solutions elsewhere. While government grants do exist, they are not available to all technologies, or technological maturities, consistently. As one industry expert stated, "Hard-tech is...hard. It is capital intensive, difficult to attract venture capitalists, and lacks a clear demand signal from the government." The government must invest additional resources to counter the ever-increasing malicious activities from adversaries.

Rigid Acquisition Practices Discourage Disruptive Innovation in Federal Government

Valley of death

The current Planning, Programming, Budget, and Execution process halts innovative concepts for two years to submit budget proposals, receive Congressional funding, and award contracts. This "valley of death" discourages innovation across the federal landscape. During recent testimony, a leading expert, describing the budget process as outdated and "preventing the flexible investment needed in prototypes, concepts, and experimentation of new concepts and technologies like AI [artificial intelligence]."[30]

Sporadic use of flexible contracting vehicles

Despite the newly released Adaptive Acquisition Framework and Congresses' encouragement to use new contracting approaches to accelerate contract awards, understanding and implementation have been sporadic across the department. Organizations such as the Defense Innovation Unit have adapted their processes to work at the speed of the commercial industry, awarding prototyping contracts in 60-90 days instead of the 18-month Department of Defense standard. Defense Innovation Unit has embraced Other Transaction Authorities that allow prototype contracts to transition to follow-on production contracts and deliver capabilities in 12-24 months.[31] The Defense Innovation Unit processes are "focused on balancing speed, flexibility, and collaboration to award prototype projects to leading-edge, dual-use technology companies that might otherwise not do business with the DoD [Department of Defense]."[32] Likewise, the Air Force Research Lab recently initiated a $1B Indefinite Delivery Indefinite Quantity contract that will expedite cyber development; similar initiatives are necessary for the United States to remain competitive and relevant within this sphere.[33] Incorporating flexibility and agility into the acquisition process will provide solutions at the "speed of cyber" to counter these dynamic, persistent threats.

Inefficient oversight and implementation of cyber tools

Across the federal government, programs procure, install, and manage a diverse set of disparate software tools for cybersecurity. Without centralized management, each organization must procure and manage its cyber software. Currently, the disconnect between piecemealed cybersecurity solutions enables the number and severity of cyberattacks. Without centralized

procurement of standardized tools, the federal government is likely paying more for these services than it could receive if it had a more centralized approach. As adversaries increase the complexity of attacks and government operations become more reliant on the IoT, this disjointed approach inhibits the U.S. government from protecting its networks.

Human Capital and STEM

Valuing diversity and inclusion increases employee morale, commitment, and productivity. However, many segments of the U.S. population are not reaching their full potential, particularly in STEM. Studies show that inequalities exist in STEM education within the African American and Hispanic communities. Additionally, these communities see disparities in career advancement opportunities in the cyber workforce. Participation in STEM education and careers is disproportionately low among African Americans and Hispanics, higher among Asians and Caucasians, and uneven among women. African Americans comprise 11% of the workforce, Hispanics 18%, but only 9% and 8% of STEM jobs. Women constitute half of the STEM jobs, 74% of health jobs but only 25% of computer jobs. Black students earned 10% and Hispanics 15% of overall undergraduate degrees in education but only 7% and 12% in STEM. Women earned 58% of bachelor's degrees but only 53% in STEM and 19% in computer science.[34] STEM graduates traditionally earn higher wages, so the above data demonstrates an important source of U.S. pay inequality. By not adequately reaching minority populations, the United States will not fully realize the power of a diverse talent pool. Lastly, the United States must recruit foreign workforce talent by establishing updated immigration policies for potential international STEM and Ph.D. students. See Appendix B for details.

Disinformation and Digital Media

The spread of disinformation by adversarial nations is a growing threat to the United States. While this weapon is not new, the speed and reach enabled by digital technologies have significantly exacerbated its impact. This national security threat is not one that the U.S. government can tackle alone. Social media platforms are increasingly grappling with preventing, removing, or tolerating illegal content or hate speech. The European Commission established a "code of practice on disinformation," and several countries are creating laws to address social media disinformation.[35] Bots have enabled malicious actors to amplify disinformation campaigns. Because the attack vector (social media and other digital platforms) and the attack surface (the general population) are squarely within the private sector, countering this threat will require a close partnership between the public and private sectors.

An International Perspective

The impact of advancements in the industry is transnational and not contained by geographical boundaries, as global economies increasingly turn digital. An increase in malicious activities and cyberattacks is a global concern that has resulted in huge losses and damages to critical infrastructures. In this respect, many countries have undertaken commendable investments to mitigate risks and secure the domain for optimal benefits.[36] The United States can leverage its allies and strategic partners to maintain its competitive advantage in this domain.

Section 3: Stakeholder Interests

Cyberspace as the fifth domain and continual advancements in computing technologies have triggered rapidly evolving challenges and obstacles that nation-states, non-state actors, non-government organizations, academia, incubators, and private businesses must keep pace or negotiate to survive. This section identifies the key stakeholders in cyberspace and the advanced computing industry, including government, industry, civil society, and international entities. While stakeholders may have conflicting interests, sometimes they align in economic growth, business opportunity and competition, security, equity, culture, sovereignty, privacy, and human rights.

Major Stakeholders and Key Sectors and Characteristics

Cyberspace and the advanced computing industry are expansive and continue to permeate daily human functions, exploration, and discovery. Key stakeholders motivated by different interests will influence changes to the future global environment. To achieve the future innovation and technology progress required, the U.S. government and advanced computing industry leaders should concentrate on the following three pillars. First, focus on digital transformation efforts, including cloud infrastructure improvements, data and analytics capabilities, cybersecurity, and business model revisions. Second, reorient and reskill the workforce to optimize remote work capabilities and capitalize on artificial intelligence, machine learning, and advanced autonomy. Finally, reexamine where and how manufacturing happens by improving transparency, flexibility, and resiliency.

Industry

Demand for cyberspace and advanced computing industries continues exponential growth due to the increasing demands of critical infrastructure, cloud and edge computing, and business and personal applications. These demands are broad, impacting hardware manufacturing locations to urban centers to every software operating system worldwide. For example, cloud and edge computing is the driving force behind the optimization of rapid data collection and analysis needs across the international spectrum, especially in energy and resources, financial services, healthcare, and government and public services.

Academia

Relationships, whether a partnership or alliance, within academia is the foundation for both the current state of intellectual advancement and the future of innovative human capital. From the U.S. perspective, America lags in the STEM disciplines compared to the great power competitors. Academia is fertile ground for fresh ideas and minds to imagine and explore collaborative basic and applied research, develop and enforce intellectual property protections, and push the boundaries of disruptive technology funded by scholarships, grants, and endowments.

Labor force

Reflecting on the transformation from steel production to education and healthcare in the city of Pittsburgh, Pennsylvania, in the mid-late 1980s, the future opportunities to reskill, reorient, and adapt to changing economic circumstances are remarkably similar in the post-COVID-19 pandemic environment. This phenomenon exists not only within the vast talent pool in the United States but also abroad. As a result of this significant shift, many interagency conversations focus on how best to reform U.S. immigration policies. Because of the unevenness of these discussions and varied outcome decisions, there is inconsistency in establishing a long-term standard to recruit, train, and incentivize human capital, both foreign and domestic. Moreover, with an aging workforce population around several global manufacturing hubs, the transparency and forward vision for transition plans to increase manufacturing automation are uneven.

Defense industrial base

In the environment of great power competition, the U.S. defense industrial base must maintain strategic technical competitiveness in cyberspace and the advanced computing industry. The defense industrial base partnership with the Department of Defense consists of more than 100,000 prime and sub-companies with domestic and foreign production assets in many countries.[37] This organism provides products and services essential to mobilize, deploy, and sustain military operations. As disruptive technologies change the character of war, the defense industrial base is beginning to sharpen its focus across the worldwide industrial complex to enable relevant and timely research and development, including design, production, delivery, and maintenance. However, patriotism and volunteerism only go so far, and the U.S. government is considering additional incentives and easier acquisition processes to expand and strengthen the defense industrial base.

U.S. government

Within the U.S. government, cyberspace and advanced computing stakeholders include Executive branch entities, departments, and agencies such as the White House, National Security Council staff, National Economic Council, Office of Science and Technology Policy, Department of Defense, United States Cyber Command, Joint Artificial Intelligence Center, the Intelligence Community organizations with cyber operations, Department of Homeland Security, Department of State, Department of Commerce, Department of Education, National Security Agency, Department of Justice and Federal Bureau of Investigation, and the U.S. Congress. The U.S. government, with partners and allies, seeks to have a fair and level playing field in cyberspace and the advanced computing industry for U.S. companies. The current primary focus is on how to best counter and challenge the outcomes from the 2020 China New Media Conference. For example, for promoting Chinese socialist values, revised history, and the export and proliferation of those same ideals across global markets and industries, the U.S. government could implement restrictions on Chinese-made products.[38]

International partners and allies

Very few international organizations are untouched by cyberspace and advanced computing platforms and infrastructure. As such, the United States should continue to be one of the foremost leaders in championing shared interoperability with those like-minded bilateral and multilateral entities. Together and separately, groups such as NATO, the United Nations and the International Telecommunication Union, European Union, African Union, Association of Southeast Asian Nations, Organization of American States, Group of Seven (known as the G7), Group of 20 (known as the G20), World Trade Organization, and others are the economic and security communities for nearly the entire globe. Therefore, safe and secure cyberspace to tackle and resolve the world's most challenging issues is the foundation for international partners and allies to cooperate, collaborate, and prosper.

Civil society

Consumers of cyberspace and advanced computing products and applications, including international consumers, expect a certain level of safety, security, fairness, privacy, honesty, and even restraint in their employment and deployment. Civil society should believe and trust in a "no harm" ethos from the usage of artificial intelligence, machine learning, deep learning, directed energy, and autonomous weapons, while building upon cyber literacy and safeguarding privacy protections of user information and data.

Coordination among diverse stakeholders

Many twenty-first century cyber challenges require whole-of-nation solutions, yet the cast of players within the cyber industry is expansive, making effective coordination increasingly difficult. Figure 2 illustrates this complicated environment. This graphic is not an all-inclusive map of the ecosystem; instead, it represents many of the organizations the Industry Study engaged with and only shows the challenge of effective coordination.

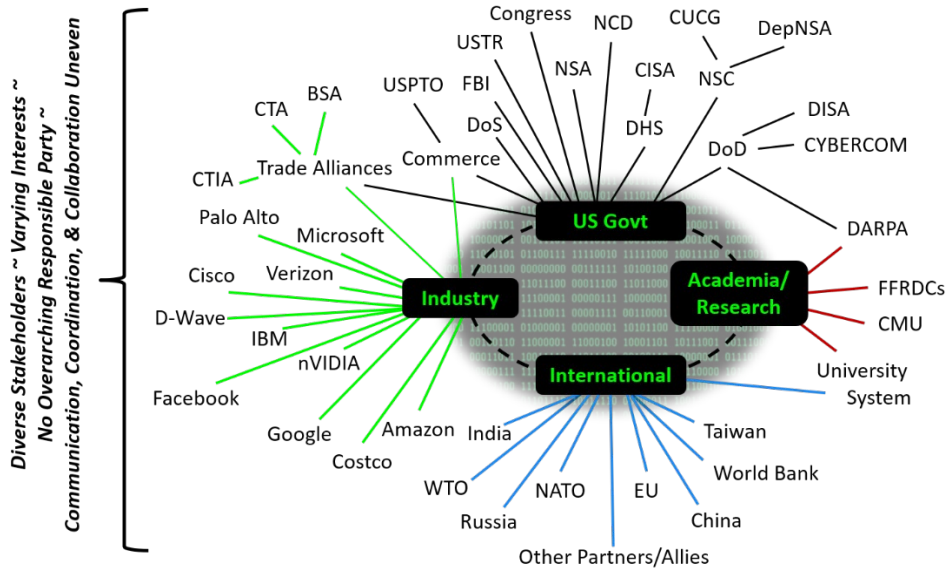

Figure 2. Visual representation of the complexity of stakeholder interactions by Kristen Wood.

Interests

Ethics

From a sovereign government perspective, there remains little consensus on forging an international framework of shared and accepted norms and values applied to cyber capabilities. Moreover, the power of advanced computing elements, such as machine learning and deep learning, enables authoritarian nation-states to expand their surveillance enterprises, further entrenching biases and lending to abuse of individual and human rights. From an industry perspective, the tension between the success of creating new, lucrative applications or breakthroughs and navigating a relatively unregulated domain and industry with ethical and moral values. An example of this might be broad support by social media companies for new regulations or legislation of their markets and products. Finally, the end-users should expect a growing need for increased cyber literacy and education to understand the potential impacts of new technologies on democracy, cultures, and ways of life, ranging from the individual to global commons.

Innovation

Innovation fuels the advanced computing industry. Companies will invest significant amounts of R&D to remain ahead of their competition and on the bleeding edge of innovation. Privacy and ethics are ill-defined on this bleeding edge, however. The United States and other like-minded nations must overcome their differences and establish standard rules governing artificial intelligence and machine learning employment. "To retain military overmatch, the United States must restore the ability to produce innovative capabilities and harness innovative technologies."[39] Persistent innovation underpins American prosperity and remains a vital interest.

Economic growth

U.S. national economic growth, in contrast to great power competitor economic growth, is a central concern for all stakeholders and a key component of business success. In this regard, civil society and private end-users should expand access to the internet and 5G telecommunications as an essential utility for work, education, social interaction, and leisure activities. This requirement necessitates greater electromagnetic spectrum allocation and management for 5G technology and beyond between the Department of Defense, the commercial/private sector, and the International Telecommunications Union. Progressive initiatives are needed to articulate and manage international rules and policies across cyberspace and the advanced computing industry. Moreover, to compete with China's advancements in quantum computing, the United States requires significant attention to encryption protocols to ensure privacy and data security.

Supply chain management is another critical component of economic growth. A supply chain with robust and resilient security reduces the exploitation of vulnerabilities, limits logistical interruptions of vital materials, and interference with hardware tampering during

manufacturing. As China continues to use increasingly aggressive and unfair mercantilist policies and programs against Taiwan, a dependent portion of the U.S. supply chain, the need for a more secure supply chain increases. The Taiwan Semiconductor Manufacturing Company and Samsung are the cutting-edge foundries of advanced chips; in 2019, China invested $29B in foundries to expand its fabrication footprint to gain an independent, secure supply line. Should China takes control of Taiwan, the controlling interest of China would be significant to the rest of the global economy, and the impacts far-reaching.

Security

Critical infrastructure, including international financial systems (e.g., New York Stock Exchange, Nasdaq, and Nikkei Stock Exchange) and other private firms across cyberspace and the advanced computing industry, are under increasing threat and attack from malign actors. The rise of ransom-based attacks, such as the ransomware attack on the U.S. firm Colonial Pipeline Company in early May 2021, and data theft are of significant concern. Maintaining robust collaboration with the Cyber Unified Coordination Group and Information Sharing and Analysis Centers to keep pace with the evolving cyber vulnerabilities and threats is necessary. However, those entities may lack the appropriate and sufficient levels of protection within the boundaries of Presidential Policy Directive 41, United States Cyber Incident Coordination.[40] The advanced computing industry should evolve on pace with the emergence of 5G infrastructure writ large, artificial intelligence, machine learning, deep learning, and quantum computing. Additionally, civil society expects an expansion of privacy and freedom of speech protections while aggressive enforcement, investigation, and prosecution of cybercrime should be the international standard and norm.

Section 4: Porter's Diamond

Introduction

The Industry Study analyzed five nations using Michael Porter's Diamond to assess the individual nation's capacity to innovate across cyberspace and the advanced computing industry. Porter's Diamond, outlined in a 1990 Harvard Business Review article titled "The Competitive Advantage of Nations," identifies four factors to help the Industry Study spotlight "sources of a nation's competitive advantage and the path to obtaining such an advantage."[41] As outlined in Porter's article, the four factors include:

- Firm Strategy, Structure, and Rivalry – Focuses on the national market as well as the nature of the domestic rivalry
- Factor Conditions – Outlines the national position in factors of production, such as skilled labor or infrastructure
- Related and Supporting Industries – Identifies the presence or absence of supplier and other related industries
- Demand Conditions – Describes the nature of home-market demand for the industry's product or services.[42]

Additionally, Porter's article includes assessing the government's role in supporting the factors within Porter's Diamond and chance.

After reviewing the cyber supply chain and emerging technologies (e.g., 5G telecommunications, IoT, artificial intelligence, quantum computing), the Industry Study selected the United States, China, Russia, Taiwan, and India for this assessment. The following sections provide key takeaways from each review as well as advantages and disadvantages for the two main themes based on an evaluation of each nation's Porter's Diamond analysis. Appendix C contains detailed assessments for each country.

United States of America

The United States remains the global leader in technological innovation despite significant competition from China, Taiwan, and India.[43] Sustained technological innovation has been, and continues to be, the fundamental element in ensuring the United States remains competitive in cyberspace and the advanced computing industry. As Michael Porter argues, "a nation's competitiveness depends on the capacity of its industry to innovate and upgrade."[44] Many factors that form the "diamond of national advantage" contribute to U.S. global leadership in cyberspace and advanced computing.[45]

Although many of these factors positively contribute to generating a systemic national advantage, specific factor conditions and elements of firm strategy, structure, and rivalry provide the greatest impact in developing a competitive advantage in cyberspace and the advanced computing industry. First, the stable and predictable regulatory environment in the United States, including the robust protection of intellectual property rights, provides the backdrop to a competitive environment with powerful rewards for innovation. Second, this regulatory

environment allows firms and individuals to capture significant portions of the value generated from innovation. This value capture, via powerful financial rewards, drives intense competition, rivalry, and innovation among tech firms, fueling perpetual technological innovation. These two primary factors facilitate many of the other elements of Porter's Diamond, such as access to capital, highly skilled labor, and business incubators, that ultimately drive cyberspace and advanced computing innovation.

As the global leader in technological innovation, the United States is increasingly in jeopardy as China is strengthening many elements across all elements of Porter's Diamond. While the United States is acting in response to this threat, there are key areas where it remains disadvantaged. First, the United States has been generally unsuccessful in establishing global norms and standards for conduct in cyberspace. The lack of international consensus on "incident response, technical standards, and law enforcement cooperation" hinders the promotion of U.S. "national interests in the realm of cyberspace."[46] Second, the United States continues to face significant supply chain risks. These supply chain risks are broad and are manifest in "manufacturing, assembly, and distribution of hardware, software, and services."[47] Of particular concern to the United States is the growing number of dual-use technologies critically reliant upon semiconductors primarily manufactured in East Asia. Although efforts are underway to reduce these competitive disadvantages, additional policies are needed to advance U.S. national interests to ensure the United States out-competes China.

People's Republic of China

In the era of great power competition, China has proven to be a significant competitor, ranked #2 globally by gross domestic product, only behind the United States. In the cybersecurity and advanced computing sectors, China's significant developments in the last 40 years revamped China's economy and created manufacturing, semiconductor, and interconnected high-technology ecosystems. China's economic power today, and likely its future growth, will also result from manufacturing and high-tech industry.[48] China, much like every other economy, has competitive advantages and disadvantages within its success. Overall, China benefits from low-cost structures and labor, skilled engineers and scientists, robust science and technology infrastructure, an enormous pool of consumers, and a cluster of sectors that feed into each other. However, as firms establish themselves in the Chinese market, they often find that the Chinese government fails to protect their intellectual property and heavily monitors and regulates data transfer. Compounding these problems, foreign workers struggle to succeed in a country with significant language barriers.

China's competitive advantage is primarily the result of firm strategies and structures and the government's human capital decisions which significantly improved its ability to compete globally.[49] China possesses an abundance of labor at low cost compared to the other global economies, landmass for building factories, and low transportation costs. These items amplify its ability to establish the necessary infrastructure and workforce to dominate its opponents through speed and flexibility and the ability to react to consumers' desires.[50] Due to its population of 1.39 billion, China has access to an enormous consumer market. Its current and evolving policies under the Chinese Communist Party party allow it to experiment, research, invest, and innovate.[51] The Chinese Communist Party's focus on human capital, specifically in the science

and engineering sectors, rejuvenated China's ability to target R&D, thereby allowing a more free-market economy and extensive investment in the digital age revolution.[52]

The Chinese government's direct investment and policies explicitly targeting the development and sustainment of advanced technology firms accelerated a Chinese digital and information age revolution seemingly overnight. China's ability to focus, promote, and build industrial parks and high-tech zones rapidly grew China's middle-class, exponentially increased its college graduates and knowledge base, and highly encouraged Chinese companies' venture capital investing in foreign companies. China's government influence on firm strategy, structure, and policies is the basis of the country's competitive advantage. Some of these same aspects of Porter's Diamond that serve as an advantage for China also present disadvantages.

China experiences some competitive disadvantages in factor conditions, and strategies, and structures. Although China has seen an increase in its number of graduates, advanced its R&D initiatives, and is the world leader in patent applications, it simultaneously struggles to protect intellectual property. The Chinese government lacks the protection of intellectual property and basic protections that foreign investors are used to and expect for their patents, innovation, and intellectual creativity. China continues to shift reforms toward better regulation and, in the last month, has pledged better protections and improved regulation.[53] However, it still has a long road ahead of it to parallel the protections global firms experience with western countries.

Additionally, the Chinese Communist Party's heavy involvement in the market and cultural sensitivities make China culturally temperamental. Firms and businesses partnering with Chinese companies will always find themselves remaining mindful of their relations, public affairs, and partnerships with other countries that could offend or upset the Chinese Communist Party, limiting or restricting their business opportunities. This hesitancy is especially prevalent when dealings involve contested areas and geopolitically sensitive disagreements (e.g., South China Sea, Tibet, Taiwan, and Hong Kong).[54] These same nuances and conscious efforts to remain culturally sensitive to the Chinese Communist Party's political stance to these contested land areas discourage international talent from going to China. Although China has loosened its immigration laws and initiated extensive recruitment programs for foreign talent, its political and cultural environment continues to serve as a competitive disadvantage, mainly due to the "centrality of political relationships in the Chinese workplace."[55] This integration of relationships ultimately benefits China's ability to implement immediate policy change but discriminates against foreign businesses.

China clearly understands its attractiveness to foreign investors and excels at highlighting these features and using them to their advantage. In the same manner, it also understands its missed opportunities and the factors yielding to these. Still, China will need to significantly change culture, governance, and business strategies to see continuous positive change in these areas.

Russian Federation

Of the five countries assessed, Russia is the weakest when evaluating Porter's Diamond for the cyberspace supply chain and emerging technology industries. The Industry Study only focused on these two themes for consistency and did not evaluate Russia's gray-zone cyberattack infrastructure or cybersecurity. "Despite possessing vast natural resources, a highly educated population, and cutting-edge technologies," Russia struggles to remain competitive.[56] Overall, Russia has many of the factors required to enable cyberspace innovation; however, the Diamond is unbalanced. The government restricts the nation's ability to fully exploit the elements and compete with the other four countries.

For the two main themes, Russia's ecosystem provides several advantages. First, Russia is in a strategic location with easy access to both Europe and China. Russia also naturally holds vast natural resources and a large population. The population is well educated, and higher technical education is available. Additionally, the Russian defense industry is strong, adding a potential link between the cyberspace domain and high-tech defense industries. Furthermore, the Russian government supports growth in the cyber industry with initiatives such as the Skolkovo Technology Innovation Center, a Silicon Valley counterpart, and the Nauka national project to bolster scientific expertise.[57] The government also advocates for emerging cyber technology R&D.

Unfortunately, the disadvantages outweigh the advantages of these two themes. First, the government inhibits growth in multiple ways. Its disruptive international behavior, cyberattacks, and efforts in Ukraine drove the United States and European Union to enact sanctions. These sanctions restrict Russian access to global markets and reduce foreign investment inside Russia.[58] Second, Russia's incredibly bureaucratic system, including massive corruption, burdensome tax laws, and restrictive business practices, limits international investment in Russia and restricts domestic performance. Third, despite a sizeable middle class and knowledgeable buyers, domestic demand remains low, leading to an inability to generate the necessary resources to invest and innovate. Fourth, Russia struggles "to retain talent in support of homegrown innovation and R&D."[59] Furthermore, the "increasingly dominant and predatory role of the state sector," along with government preference for State-Owned Enterprises versus private companies, restricts competition.[60] All of these disadvantages offset the advantages, limiting Russia's ability to compete on the global stage.

Taiwan

Taiwan is entering the stage of innovation-driven economic growth, according to a World Economic Forum assessment.[61] For a country to enjoy sustainable economic growth and stay competitive internationally, the key lies in the government's investment in R&D to drive technology breakthroughs and innovations and effective resource integration.[62] As such, the government targets "innovation, employment and equitable distribution" for Taiwan's future development needs.[63] Taiwan's "five plus two" initiative focuses on five industries and two projects to improve innovation. The industries include intelligent machinery, the IoT (the Asia Silicon Valley Plan), green energy, biomedicine, and national defense and aerospace. The two projects include circular economy and new agriculture as innovative economic models for

sustainable development to create high-quality jobs, raise incomes, and genuinely realize equitable distribution of employment through innovation-driven economic growth.[64] Porter's Diamond framework analysis highlights several advantages and disadvantages when assessing Taiwan's competitiveness.

Taiwan's competitive advantage continues to flourish through factor and demand conditions. Taiwan adapted its strategy from Made *in* Taiwan to Made *by* Taiwan to increase its competitive advantage. Taiwan leads the global semiconductor industry and leverages innovative technologies (e.g., 5G telecommunication, IoT, artificial intelligence, and machine learning) to gain a global advantage. Taiwan is rich with human resources and a highly skilled and educated workforce. Pursuing new economic growth momentum through innovation and structural reform measures is key to Taiwan. The "five plus two" industry innovation plan, outlined previously, aims to spark innovation and spur the trend of industry innovation by developing application services based on the foundation of the existing cyber industry. The industries within the plan highly link to one another, and their success will also spread benefits to a wide range of other industries.[65] Globally, the demand for semiconductors rose with the virtualization of businesses during the COVID-19 pandemic. However, the demand exceeded Taiwanese capabilities and resulted in global shortages of semiconductor components. Domestically in Taiwan, consumer spending began to rise as the country started recovering from the COVID-19 pandemic, which unexpectedly further increased the virtualization of businesses.

The role of government and factor conditions play a part in the disadvantages impacting Taiwan's competitiveness. China's ongoing attempts to isolate Taiwan diplomatically threaten its long-term political autonomy and its ability to maintain its presence in overseas markets.[66] U.S. and Taiwan relations are increasingly important strategically. A competitive manufacturing sector encompassing electronics, machinery, petrochemicals, and information and communication technology products drives Taiwan's trade-dependent economy. Factor conditions are also a disadvantage. Taiwan faces significant obstacles in its effort to ensure a robust and growing STEM talent pool amid international competition, especially from mainland China.[67] Studies show Taiwan saw diminished connections to Silicon Valley in the 2000s for two reasons: first, with more opportunities at home, fewer students from Taiwan came to the United States to study; second, Silicon Valley firms like Apple increasingly partnered with lower-cost Chinese, not Taiwanese, firms for their manufacturing needs.[68] In addition to the challenges with China, Taiwan also has to factor in aging workforce issues.

In all, Taiwan seeks innovative-driven economic growth to maintain its competitive advantage. Government policies such as the "five plus two" initiative provide Taiwan a pathway as they face challenges with an aging workforce to continue its pursuit for the future.

Republic of India

India is a central player in the digital technology sector. India's Information Technology and Information Technology Enabled Services account for 55% of the total global outsourcing market, and the country is the premier offshoring destination for global technology companies.[69] Additionally, Information Technology and Information Technology Enabled Services make up 8% of India's gross domestic product, and the technology industry is the largest private-sector

employer in the nation.[70] While India has historically focused on information technology services and software, there is a nascent yet growing shift toward hardware. The performance of these industries and commensurate non-tech sector growth within India led economists to project that India will become the fifth-largest economy in the world by 2024.[71] Viewing these factors through the Porter's Diamond lens can help provide insight into India's national competitive advantage.

The primary driver of India's competitive advantage is its Factor Conditions. The country enjoys an ample supply of low-cost, young, educated labor. India is the second-largest English-speaking nation globally and has the highest graduation rate of engineers, trailing only China.[72] The Indian culture is known for "resourcefulness," which feeds into a growing entrepreneurial sector. Demand conditions – both internal and external – also provide a competitive edge. Internally, India is one of the largest and fastest-growing digital consumers on the planet. India has over 560 million internet subscribers but only accounts for less than half of the population, leaving significant room to grow.[73] Externally, many Multi-National Corporations and tech firms have subsidiaries in India, further fueling demand. A few large corporations characterize India's industry structure on top with many smaller businesses below. This pyramid structure encourages competition and innovation; most firms compete through niche-market strategies to set themselves apart from their competitors and embrace any competitive advantage available to them.

India faces various disadvantages that it must overcome if it is to reach its full digital potential. First, ubiquitous bureaucracy and red tape hinder the Indian government. Some see India's rise in the technology industry to be despite, not because of, the Indian government. While India does have a relatively educated population with a solid education structure, the education system needs reform to address capacity issues and lack of access in rural areas with such a large, young population.[74] India still has many regions considered "developing," and there is a growing need for infrastructure improvements. The lack of reliable infrastructure is one reason for India's focus on software – the cost of entry in terms of infrastructure for a software firm is much lower than that for a hardware firm.

Overall though, India is on an upward trajectory of growth and prosperity. Their "Make in India" and "Digital India" programs are deliberate strategies to continue this growth, and the government has declared "technology" to be one of twelve champion service sectors.[75] There are challenges that India's public and private sectors must embrace and overcome. However, in so doing, the factor conditions, demand conditions, firm strategies, and related industries will help cultivate a continued competitive advantage for this emerging nation.

Porter's Diamond Analysis and Conclusions

These five Porter's Diamond assessments spotlight the United States, China, and Taiwan as the primary players within cyberspace and the advanced computing industry. Both the United States and China provide a comprehensive innovation ecosystem approach, channeling government policy to support all four factors within the Diamond. In the cyber supply chain industry, Taiwan delivers a unique ecosystem. Their focus on emerging technology to improve innovation across the spectrum looks promising for future growth. While not at the same scale as

the United States, China, or Taiwan, both Russia and India have unique niche factors. Russia's strategic location and large, well-educated population offer significant advantages; however, their government behavior inhibits progress. India is already a major player in the related information technology services industry, has a large educated population, and actively pursues policies to improve its innovation base and drive growth. While the United States maintains some advantages across the four factors, it no longer retains a sole competitive advantage in the high technology arena. This assessment outlined a holistic look at the entire ecosystem within the individual nations. The following section evaluates the Strengths, Weaknesses, Opportunities, and Threats for each country.

Section 5: Strengths Weaknesses Opportunities Threats Analysis

To remain a preeminent force within the great power competition, the United States must frequently and thoroughly examine the strategic factors concerning SWOT for its near-peer adversaries and allies related to operations in cyberspace. Identifying and mitigating critical risks associated with cyber threats and weakness while capitalizing on strengths and opportunities allows the United States to assess its standing within this domain continually. Chinese companies have caught up to and surpassed the United States in some fields. Russia and China have fully integrated cyber warfare capabilities into their policy toolsets. They have the industrial and technical cyberspace and advanced computing capabilities to challenge the United States and its partners and allies. While a software powerhouse with a huge untapped domestic market, India has not yet developed the manufacturing capabilities needed to challenge China.[76] Taiwan is strategically vital as the world's supplier of advanced semi-conductor chips; increasing tensions with China exacerbate U.S. supply chain vulnerabilities. Based on the SWOT analysis findings, the United States needs a more robust human capital pipeline, a whole-of-nation strategy, and improved capabilities to quickly solve supply-chain and innovation issues to enable a more robust cyber defense posture.

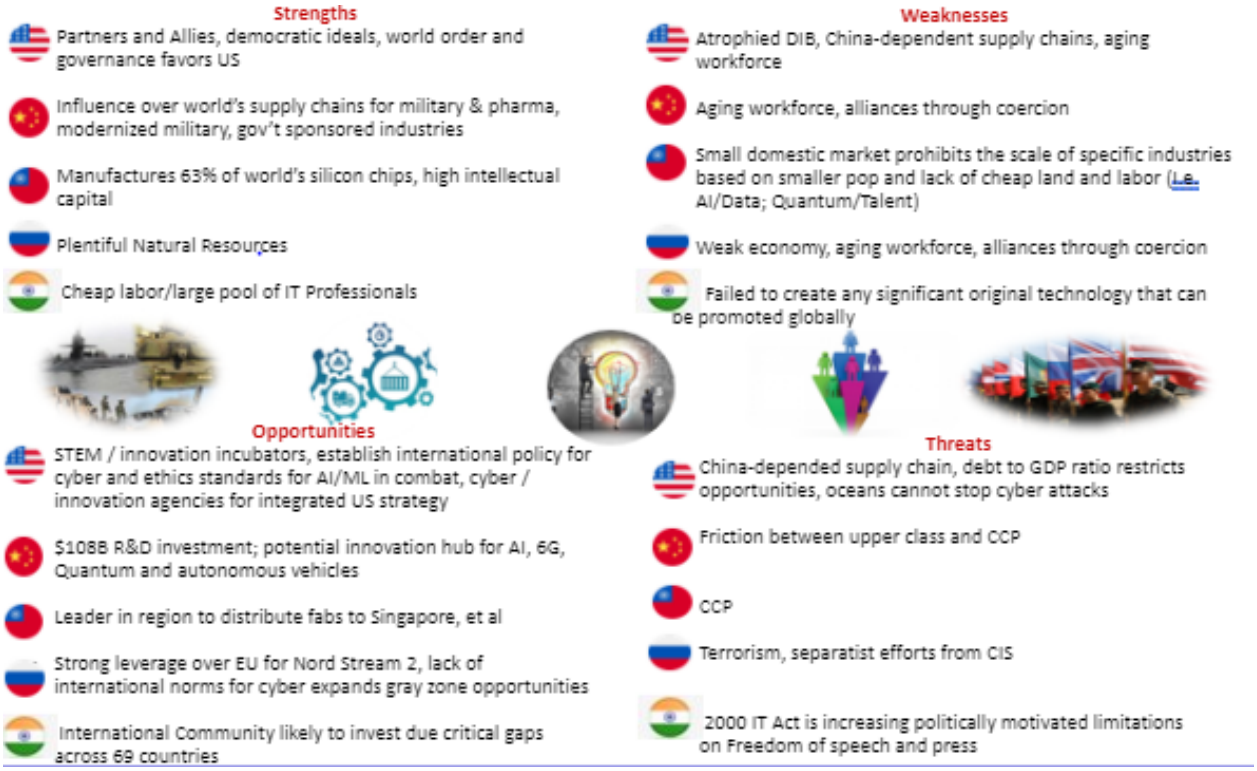

Figure 3. SWOT Analysis of the United States, China, Taiwan, Russian, and India by Laverne Amara and Heather Putman.

Section 6: Outlook – Future of the Industry

Multiple interrelated factors will shape cyberspace and the advanced computing industry in the future. The industry will continue to grow exponentially as technological advancements in the advanced computing industry, like quantum computing and blockchain technology, exacerbate existing cybersecurity vulnerabilities. These vulnerabilities are not solely related to the advancing technology, but by the increasing connectedness through internet of things (IoT) devices globally. By the end of 2018, there were an estimated 22 billion IoT-connected devices. Forecasts suggest that by 2030 around 50 billion of these IoT devices will be in use worldwide, creating a massive web of interconnected devices spanning everything from smartphones to kitchen appliances.[77] There will be increased competition for limited resources (human capital, rare earth elements) that will have cascading effects through the supply chain in critical industries on a nation-state level.

There are several developments on the global stage affecting the future cyberspace environment. 5G telecommunications will underpin the internet economy and provide the backbone for the next generation of digital technologies. Therefore, it is unsurprising that there is intense competition among companies and countries for 5G telecommunications leadership, as seen in Appendix D.[78]

Furthermore, the limited number of firms in the semiconductor supply chain has led to undesired effects, such as higher costs, inferior quality, and higher risk of compromised products (e.g., integrated circuit backdoors, counterfeits, and clones). In terms of opportunities, exponential advancements in computing power and speed will likely continue unabated, increasing opportunities to solve complex problems.

A U.S. Perspective

From the U.S. perspective, there are various desirable outcomes for establishing competitive advantages in cyberspace and the advanced computing industries. Quantum computing and manufacturing present opportunities for the United States to leverage other technologies such as blockchain. Blockchain has two relevant applications concerning quantum. Firstly, cryptographic experts believe quantum computing will break the public key encryption used in some blockchain technology.[79] However, blockchain solutions are now implementing quantum-proof cryptographic algorithms.[80] This fusion of seemingly disparate technologies demonstrates the importance of leveraging other advanced computing fields and recognizing their impact on each other in the future. Secondly, concerning great power competitors, China and Russia view blockchain as a central and transformative technology and are taking actions to bring its promise to fruition. Chinese President Xi Jinping announced his intention to use blockchain to gain "a new industrial advantage." China appears now to be outpacing America in blockchain patents.[81] In 2018, Russia's intelligence agency, known as the FSB, stated, "the Internet belongs to the Americans – but blockchain will belong to us."[82] Russia and China seek to set standards on blockchain by adopting it faster than the United States and sending large amounts of delegates to international forums working on blockchains, such as the International Standards Organization and International Telecommunications Union.[83] Leveraging advanced computing will enhance secure, resilient, and safe domains that encourage innovation and

technology advancement. Additionally, internationally accepted and precise definitions of a structured and standardized threat, accountability, and attribution will benefit the United States by promoting a stable and secure supply chain protected from geopolitical conflicts.

Within cyberspace, several other dynamics are emerging. Artificial Intelligence, Machine Learning, and High-Performance Computing are starting to demonstrate broad application across multiple industries as they become general-purpose technologies with broad economic impact. Firm acquisitions will likely continue to progress as firms vertically integrate to acquire specialty developers. An example of this is Microsoft's acquisition of CyberX (IoT cybersecurity firm). Microsoft plans to integrate the technology into its business-related Industrial Cybersecurity to minimize cyber threats on IoT technologies used in the manufacturing field. Also, it may integrate the technology with its cloud products having IoT support.[84] Acquisitions such as these may continue with larger firms acquiring smaller firms for their skilled cybersecurity labor.

Several recent attacks have demonstrated that on-premise servers can be equally or more vulnerable than managing data in the cloud. The industry offers many off-the-shelf cloud solutions approved by the Federal Risk and Authorization Management Program (FedRAMP), including Amazon Web Services (AWS) GovCloud, Microsoft Office 365 and Azure, IBM SmartCloud, and Salesforce Government Cloud. Many federal and state agencies already have migrated to cloud solutions, achieving National Institute of Standards and Technology (known as NIST) authorization and demonstrating the effectiveness of cloud management. Department of Defense specifically launched its Joint Enterprise Defense Infrastructure (known as JEDI) Cloud acquisition program to provide cloud service to support Unclassified, Secret, and Top Secret requirements. DISA's milCloud 2.0 offers a suite of integrated cloud-based services. However, most of the Department of Defense's cloud solutions are still disparate, cannot communicate with one another, and are still not fully implemented. Benefits of cloud solutions include reduced hardware needs, reduced operational costs, standardized and thoroughly tested software, dedicated management of offsite cloud servers, and the use of artificial intelligence, IoT, and edge computing. With Platform as a Service, for example, the service provider hosts servers, networks, storage, operating system, and databases at its data center, while the government agency maintains control of the applications, configurations, and data.

The National Security Agency issued guidance on February 25, 2021, strongly recommending that defense agencies and contractors set up a zero trust security model on all critical Department of Defense networks and defense industrial base systems. The National Security Agency explained in its release that zero trust "can prevent the abuse of compromised user credentials, remote exploitation, or insider threats, and even mitigate effects of supply chain malicious activity." A zero trust architecture moves away from static network perimeters to a more dynamic, risk-based access control architecture that considers all users as potential threats and requires authentication of every user before granting access. The National Cybersecurity Center of Excellence collaborates with industry, including cybersecurity vendors, to address the challenge of implementing a zero trust architecture by sharing information and exchanging best practices.

The projection of advanced computing adoption has various effects on national security interests and the Department of Defense. Further democratization of hardware and software will

make powerful tools accessible to almost anyone, including non-state actors like transnational criminal organizations and radicalized "lone wolves." Blockchain advancement will increase organizational adoption rates. For example, potential Department of Defense uses for blockchain include accelerating procurement, enhancing supply chains, cybersecurity solutions for access, monitoring, and authenticity. Additionally, it can increase the speed, automation, and coordination of any activity, including automation of the chain of command for authorizing signatories for operational logistics and the onboarding and transfer of personnel.[85] To capitalize on the efficiencies created by blockchain and stay ahead of China and Russia, the United States, specifically the Defense Department, should mandate training, invest in, and implement blockchain technology.[86] Other considerations include growing asymmetric advantages throughout cyberspace, innovation outpacing national strategy and the U.S. government's ability to regulate, and virtualization providing key advantages in collaboration, new product development, and wargaming.

An International Perspective

Generally, U.S. partners and allies share the American assessment of the strategic environment and recognize the cyber threats posed by China, Russia, Iran, and North Korea. However, due to Russia's geographic location and the effectiveness of its cyberattacks in the region, European countries recognize Russia as a more dangerous country than China. Additionally, Iran and North Korea are not a direct threat to Europe's stability, so it is not a primary concern at this time. Such a difference in threat interpretation might result in European countries being more interested in cooperation against deterring Russia before other US competitors. Developing regions, such as the African continent, have limited cybersecurity infrastructure due to budget constraints. Despite awareness of existing threats, most developing countries prioritize increased connectivity over network security. Nevertheless, even with slightly different threat prioritization, there is solid ground for cooperation among the United States and its allies and partners on counter cyber threats. Overall, there is broad understanding and support for American initiatives to counter adversarial countries in cyberspace.

Section 7: Government – Goals and Role

Government Goals

The Interim National Security Strategic Guidance outlines the U.S. government's primary goal. The United States must "reinvest in retaining our scientific and technological edge and once again lead, working alongside our partners to establish the new rules and practices that will allow us to seize the opportunities that advances in technology present."[87] The government may establish domestic policy and pass legislation to achieve this goal domestically. In parallel, the United States must lead internationally to create international norms that benefit democratic partners and allies.

Government Role

Domestically

The U.S. government should establish cyberspace and innovation agencies to develop and implement domestic policy. These agencies can work with the Labor Department to develop and recruit for a diverse cyber workforce while working with the Department of Homeland Security to establish immigration policies to support U.S. economic interests. In concert with state and local governments, the U.S. government could attract semiconductor manufacturing factories to improve the U.S. economy by creating jobs and stabilizing supply chains. The state of Arizona recently committed to spending $205M in infrastructure improvements to incentivize the Taiwan Semiconductor Manufacturing Company to build a new semiconductor fabrication plant in Pheonix.[88] Arizona anticipates creating over 1,900 full-time jobs between 2021 and 2024. The Biden Administration's proposed infrastructure bill, if approved, could provide federal subsidies to Taiwan Semiconductor Manufacturing Company and other companies to incentivize the creation of other U.S.-based fabrication plants.

The government influences innovation by financing science and technology, innovation incubators, and STEM vocational schools through borrowing, bonds, tax increases, and incentives for private sector investment. Concurrently, the government may offer tax incentives for U.S. companies who invest heavily in R&D, achieve goals for a carbon-neutral footprint, or sponsor interns from local STEM schools. Government tariffs can either encourage or discourage companies from manufacturing in the United States. For example, "in 2018, the United States imposed a 25% tariff on U.S. imports of semiconductors and other goods from China following a Section 301 investigation into China's unfair trade practices. Since 60% of U.S. semiconductor imports from China are originally made in the United States, distributed through global supply chains, and imported by U.S. companies for themselves, U.S. chipmakers have borne the brunt of the $750 million in duties paid on chip imports since July 2018" and projected to cost as many as 40,000 jobs in the semiconductor industry.[89] Funding for these initiatives need not come solely from federal taxes; the government could also encourage private investment for Science and Technology efforts and collaborate with state and local governments and academia to accelerate the formation of innovation incubators.[90] The government has many opportunities for action and influence through policy, funding, and corporate incentives to achieve a competitive advantage

in cyberspace and the advanced computing industry. However, as underscored by this analysis, the U.S. government must act swiftly.

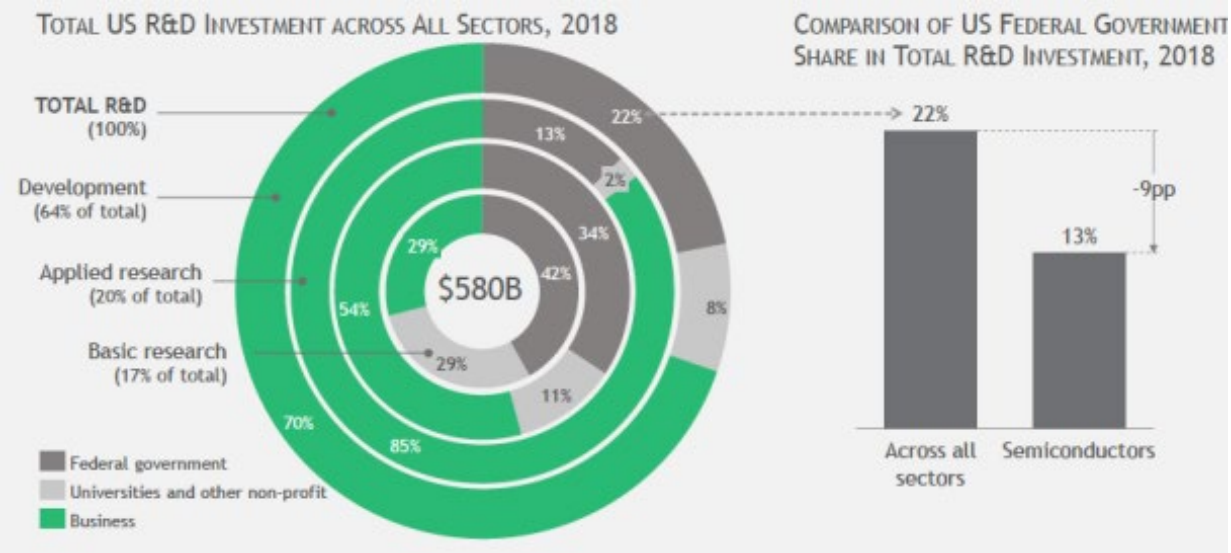

Figure 4 Comparison of R&D funding across all U.S. sectors by the Semiconductor Industry Association.[91]

Internationally

International entities such as the International Telecommunications Union, the World Radiocommunication Conference, or the United Nations Group of Governmental Experts enable collaboration with partners and allies to define international law in cyberspace and advanced computing industries. The offices of cyberspace and innovation would collaborate internationally in concert with the State, Commerce, and Treasury Departments. Their focus would range from cryptocurrency to sanctions to international trade agreements. In artificial intelligence and machine learning, where biases could create devastating outcomes, the U.S. government can collaborate to establish global standards to define the ethical use of artificial intelligence for commercial and military. Finally, the government has roles that benefit U.S. industries and the economy by providing trade agreements outside the Americas, similar to the United States-Mexico-Canada Free Trade Agreement, to increase the availability of markets. The U.S. government may also levy tariffs, impose sanctions, or require licenses to regulate trade with specific countries.

Improving market efficiency

The government must maintain a balance to improve market efficiency without injecting significant market externalities that mask demand signals or hinder a free market economy. To improve market efficiency, especially in areas such as the costly and drastic shortage of chips, the United States Trade Representative could negotiate agreements with foreign nations to establish and facilitate trade and investment opportunities for critical technology. This effort would assist the silicon chip market find a new equilibrium and guard against future supply shocks in the face of ever-increasing demand.

Distorted government support

The government's efforts to spur innovation could have negative implications. Too much government spending could artificially save companies that otherwise would, and likely should, fail due to inefficient practices. At times, the Department of Defense has selected incumbent members of the Defense Industrial Base over more innovative startup companies to ensure the country can mobilize for war. The result: this action forces startup companies out of business or discourages small companies from partnering with the Department of Defense. These actions create negative externalities, undermine efficiency, and hinder innovation.[92] The government must act now but remain cautious not to skew or distort markets improperly.

Response to challenges

Adversarial countries and non-nation state actors continue to increase their attacks, specifically in cyberspace. To best deal with these adversaries, the United States usually aligns its policies with partners, allies, and international bodies such as the World Bank and the United Nations. Collaborations on cybersecurity could include multi-nation accords or agreements. Since the United States is no longer the sole superpower in a unipolar world, the ability of the United States to counter gray-zone attacks will be more potent if it can develop consensus and collective action among like-minded nations.

Section 8: Policy Recommendations

Based on the above background and analysis, the U.S. government should address Cyberspace and Advanced Computing policy through six primary recommendations. Concentrating on these six areas provides multiple options to U.S. policymakers and ensures the United States maintains a competitive advantage in this critical warfighting domain.

1. Develop and Implement National Cyber and Innovation Strategies and Coordination

National Cyber Director should lead the development of national cyber strategy and interagency coordination

In its report, the Cyber Solarium Commission recommended that a new National Cyber Director lead the development of a national U.S. cyber strategy. In addition, the newly established National Cyber Director should provide coordination between the interagency and the U.S. private sector, focus specifically on establishing needed cyber policies, identify priority areas for coordinated government action, and define U.S. government roles, responsibilities, and standards.

Establish a national cyber center to facilitate public-private coordination

The National Cyber Director should establish a National Cyber Center to serve as a resource for whole-of-nation coordination for cybersecurity operations.[93] The Center will maintain an ongoing dialogue with stakeholders, share information and best practices, and develop recommendations for U.S. policies and initiatives. Consultations and facilitated communications would accelerate the identification of R&D projects for dual-use technologies, sharing best practices, and the cross-utilization of talent and ideas. The Center should recommend funding priorities for the U.S. government to provide the genesis for seed-funding public-private partnerships specific to cyberspace. In addition, the National Cyber Center should also develop a National Cyber Reserve of volunteers to facilitate on-demand coordination to address emerging threats and resolve specific projects and tasks. Participants should include representatives from the U.S. interagency, commercial sector, industry associations, academics, think tanks, non-government organizations, and other willing stakeholders to implement the task force's proposed recommendations and national strategy.

Priority cyber areas for further review and development

To capitalize on *blockchain technology* and stay ahead of China and Russia, the United States and the Department of Defense should maintain R&D efforts and mandate training Department of Defense experts in blockchain technology.[94] All federal government agencies should prioritize *cloud solutions* for security and effective data management following the examples of those who have migrated the technology successfully. Federal government agencies also should follow the National Security Agency's guidance and adopt a *zero trust architecture*. Blockchain, cloud solutions, and zero trust best practices should be central to the National Cyber Center's agenda for engagement and collaboration with the advanced computing industry.

Establish a national innovation director and agency

The most effective way to implement a national innovation strategy is to create a new agency. A well-respected leader with experience fostering entrepreneurship and innovation in the private sector would be most effective in leading this agency. This leader must have cabinet-level status and a corresponding title, such as National Innovation Director, to ensure sufficient influence. The Defense Innovation Board recommended such a position within the Department of Defense.[95] Interagency coordination with the U.S. private sector is needed. A National Innovation Advisor should focus specifically on promoting innovation and entrepreneurship while coordinating closely with the Office of Science and Technology Policy and National Cyber Director to support the efforts to advance strategic technologies.

Develop an innovation task force, recommendations, and a comprehensive strategy

The best approach to launch a national effort to promote innovation is to develop a comprehensive national strategy. The White House should establish a task force that includes stakeholders from the public and private sectors, including academia and civil society, to develop the strategy. Once the task force develops a strategy, the National Innovation Director should create an advisory board for collaboration. (See Appendix E for more detail.)

Launch a communications campaign to articulate the need for innovation and STEM

The U.S. government must develop an effective marketing campaign to help U.S. citizens understand the strategic importance of innovation and STEM. The message must come from the top to be considered a national priority. President Biden highlighted the need to improve U.S. competitiveness in his first address to Congress on April 29, 2021, stating: "We're falling behind the competition with the rest of the world." He added that "China and other countries are closing in fast. We have to develop and dominate" the future technologies.[96] The administration should go further by defining how STEM-related study, R&D, and innovation will lead to long-term U.S. prosperity and security and clarify how Americans can participate in the STEM economy. The National Security Council and White House Office of Science and Technology Policy should mandate all U.S. agencies develop innovation, STEM, and cybersecurity strategies for the administration's first comprehensive National Security Strategy.[97]

2. Leverage and Strengthen Public-Private Collaboration

Develop and strengthen public-private partnerships

U.S. science and technology agencies and universities should seek to develop public-private partnerships with industry leaders to deepen innovation and research specific projects of interest to the U.S. government. One immediate action is to leverage and increase funding for innovative organizations within the U.S. government, such as the Defense Advanced Research Projects Agency, the Department of Energy, and national labs. The U.S. government should also incentivize universities and U.S. companies to establish incubators and accelerators on university campuses.

Establish a Joint Public-Private Task Force – Disinformation (JPPTF-D)

A task force aligned under the National Cyber Director with representatives from the federal government, the "attention economy," and academia must work together to mitigate this existential threat. The task force should focus on combatting malign foreign influence, developing standards for fact-checking institutions such as news agencies and other non-governmental organizations, policy guidance on social media censorship, digital literacy, and other topics of increased public interest.

Support innovation clusters

Technology clusters, such as those located in Carnegie-Mellon, Silicon Valley, Austin, and others, provide an excellent model to improve collaboration, communication, networking, and ultimately draw talent, especially when industry leaders are already nearby.[98] The U.S. government should provide incentives to private industry, universities, and civil society to establish and strengthen innovation clusters. The U.S. government should also incentivize universities and U.S. companies to establish incubators and accelerators on university campuses. These initiatives will spur increased innovation, entrepreneurship, and provide capital to develop talent and nascent technologies.

Target assistance to small and medium enterprises

Before the COVID-19 pandemic, small and medium enterprises employed almost 59 million people in the United States, just over 47% of the workforce.[99] The federal government should reduce barriers to information and resources for budding small and medium enterprises. The Small Business Administration should conduct better awareness-raising campaigns, broaden its network of providers, promote workshops, short-term training, and even help develop courses at U.S. community colleges. The Small Business Administration should develop more resources to assist budding STEM-related enterprises, such as invention and technology patents. The Small Business Administration should support STEM-focused ecosystems through expanded public seed funding programs (see Appendix E on Small Business Administration programs), and tax credits. Additionally, they should work with incubators, accelerators, and banks to make Small Business Administration-guaranteed funding less risk-averse.

3. Strengthen and Leverage Alliances and International Partnerships While Establishing International Norms in Cybersecurity and Emerging Technologies

Develop and strengthen strategic partnerships in each region

The United States should develop a collaboration strategy with its strategic allies and partners to leverage the collective strengths to ensure security for the United States and its allies. The U.S. government and Department of Defense should lead an initiative to identify the strengths and weaknesses of NATO allies and partners in defense-applied technology and the development of critical emerging technologies. In the Indo-Pacific, the United States should strengthen the Quadrilateral Security Dialogue with Japan, Australia, and India. This dialogue should establish cooperation in cybersecurity and trade and investment in emerging technologies.

The U.S. government should spur trade and investment partnerships with East Asian countries in technology, especially to secure critical supply chains.

Establish strongly supported international norms

The United States should lead the discussion and elaboration of international norms for the ethical use of emerging technologies, especially artificial intelligence and autonomous machines for military and commercial use. The United States should negotiate international rules of the road and support new international institutions to detect, monitor, and help manage responses to cyberattacks. International agreements and institutions will clarify norms, increase communication, improve attribution, and reduce the risk of escalation from gray zone cyberattacks to full-blown kinetic conflict. The Tallinn Manual 2.0, completed by the NATO Cooperative Cyber Defense Centre of Excellence (CCDCE), is an excellent tool for policy and legal experts from 34 NATO and other like-minded countries to define how international law applies to cyber operations. The United States should support and participate in the Tallinn 3.0 project updating version 2.0 to focus on States' practice and statements on cyber law.[100]

4. Attract, Develop, and Retain Human Capital

Attracting talent and human capital

Promote STEM careers. The Department of Education should launch a campaign targeting U.S. schools to promote the study and raise awareness of STEM careers, both in government and the commercial sector. The U.S. government should support increased university student internships and offer tax incentives for U.S. companies to do the same. These initiatives will improve the bottom line and reputations of participating universities and provide their students with practical, real-world experience. Increasing awareness and opportunity to experience STEM early will draw more interest in youth to pursue STEM careers.

Incentivize private sector and educational outreach in diverse communities. The U.S. government should incentivize universities to implement policies and demonstrate practical outreach efforts to underserved communities to attract a diverse workforce. The Department of Education should work with states to identify and assist underserved communities and populations within the United States to provide early childhood education programs. The Biden administration's American Jobs Plan provides $100B towards modernizing public schools and early learning centers.[101] However, the U.S. government must work with state and local governments to identify the locations of greatest need.

Centralize the application process for international students. Many potential students would like to study in the United States but do not because of too many barriers. They could bring much-needed talent, but many pursue their education elsewhere. One such barrier is decentralized admissions. The Department of Education should work with the still-nascent Common App program, the American Council of Education, the Institute of International Education, and other education organizations to standardize one application process to assist with international and U.S. student placement.[102]

Developing human capital

Develop Department of Defense's cyber workforce through specialized educational programs. Three strategic options to cultivate high-quality information technology and cybersecurity military segments within the Department of Defense cyber workforce are: military education, talent acquisition, and specialized college programs. Although combining the options would produce the greatest results, military education will yield the best returns over time. The Department of Defense should enhance the existing military cyber workforce through military education and integrate specialized college programs into the Professional Military Education (PME) curriculum.

Improve teaching practices and establish measurable standards in science and technology. The U.S. government should promote innovation, improved curricula, and core standards in science and technology in lower, middle, and high schools. While 41 states and the District of Columbia adopted the Common Core State Standards for math, English language, arts, and literacy, they need to include science and technology.[103] Achieve, a nonprofit education organization that developed academic standards for over two decades and created "Next Generation Science Standards" in collaboration with many states.[104] The Department of Education should incentivize states to adopt these standards and statewide assessment practices within a given timeline, such as in two to three years.

Promote Science, Technology, Engineering, Arts, Mathematics in the classroom. Schools should invest in incorporating learning environments such as Makerspaces to foster entrepreneurship and innovation. Inclusion of the Arts with STEM education is necessary, also known as STEAM. Students who develop entrepreneurial skills "have a higher probability of success making a living practicing their art form" and create economic and social value by creating small businesses creative solutions to social problems.[105]

Increase funding for science agencies. To understand the challenges for universities to improve their programs and research, the U.S. government should meet with universities with well-developed study and research programs in technologies such as artificial intelligence, big data, quantum computing, nano, robotics, and cybersecurity. The U.S. government should also increase funding for the National Science Foundation, National Institute of Standards and Technology, National Institutes of Health, and similar agencies to coordinate R&D in these same technologies at U.S. universities. On March 31, 2021, the White House announced its American Jobs Plan, dedicating an unprecedented public investment of $270 billion in U.S. education and STEM programs, but this is disproportionately low (17.5%) compared to over $2.2 trillion to be spent over ten years. It is necessary to restructure the overall investment to dedicate 20% (an increase of over $55B) toward education and STEM to ensure long-term U.S. competitiveness. (See Appendix E for the breakdown on new public spending on education and STEM.)

Incentivize community colleges to provide worker retraining. The U.S. government should fund programs developed by community colleges to quickly start workforce training in much-needed technologies and bring manufacturing to the United States. U.S. companies can help define what skills are needed and work with community colleges to develop curricula based on international training and certification programs that many large companies have

implemented internally. Some countries also offer long-term, paid internships that develop trade, and a similar industry certification program in the United States would be very beneficial.

Retaining talent and human capital

Facilitate work visas for international talent educated in the United States. The U.S. government should work with Congress to update U.S. immigration policies to provide incentives to prospective international students and researchers to seek long-term, gainful employment in the United States. The Biden administration sent a bill to Congress on January 20, 2021, to make it "easier for graduates of U.S. universities with advanced STEM degrees to stay in the United States" while they look for employment, and Section 3401 of the bill exempts them from the numerical limits on green cards.[106] The bill specifies that this exemption is for Ph.D. STEM graduates only. Legislation to attract STEM talent should go much further by including Master's graduates and removing work visa limits for employers to hire increased foreign talent given the appropriate labor need.

Update immigration laws specific to strategic sectors. Providing a fast-track to STEM labor certification to work in the United States is an essential first step. The White House should work with Congress to update U.S. immigration laws to retain foreign talent by establishing a predefined pathway to naturalization for those who have studied or worked in the United States in pre-identified science and technology sectors. (See Appendix E on overcoming risks of intellectual property espionage and job displacement.)

Incorporate innovation best practices in government – diversity, innovation culture, and improved personnel services.

The federal government must continue to develop a work environment that respects and leverages diversity, promotes and rewards innovation, and improves personnel services. (See Appendix E for the description of these best practices.)

5. Strengthen Supply Chains in Strategic Technologies and Infrastructure

Develop resilient U.S. supply chains

To strengthen the resilience of U.S. supply chains, the White House issued an Executive Order on February 24, 2021, laying out its strategy on supply chains and requesting U.S. agencies to identify critical supply chain vulnerabilities and develop proposals on how to address them.[107] The U.S. government should support U.S. companies to establish and develop manufacturing operations in the United States. The U.S. government should provide investments and tax incentives to companies, encourage city and state governments to provide incentives, and develop innovation ecosystems for human capital and infrastructure.

As U.S. agencies assess the risks and opportunities of various supply chains, the U.S. government must ensure secure critical sector supply chains, such as the semiconductor industry and medical supplies, like combating the COVID-19 pandemic. As needed, Congress should invoke the Defense Production Act to address immediate shortages and facilitate immediate

production. For example, the White House held a "chip summit" with semiconductor and automotive industry leaders. Intel and Taiwan Semiconductor Manufacturing Company announced construction projects for semiconductor fabrication plants in Arizona, and Samsung and Micron are considering onshoring future fabrication plants.

Pursue trade and investment agreements in critical technologies and supply chains with strategic partner countries

The U.S. government should strike mutually beneficial trade and investment agreements with Taiwan, South Korea, Japan, and the Netherlands to advance joint commercial and security interests in the semiconductor industry and associated supply chains. These agreements presented as sound economic policy vs. political. These agreements will strengthen supply chains and increase trade and investment with more secure and resilient countries that support democratic and free-market economic policies. Taiwan already has a substantial market share and human capital of the semiconductor industry and well-developed technology ecosystems, working to move the physical to virtual innovation and collaboration in the future.

6. Modernize U.S. Defense Structure by Leveraging Streamlined Acquisition Processes, Assigning Appropriate Funding to Adopt Emerging Technologies

The Department of Defense should allocate a minimum of 20 percent of its RDT&E budget for science and technology (disruptive innovation)

The government should mirror leading commercial industry partners who invest 29% of their R&D on disruptive innovation on average to reflect an industry best practice.[108] Specifically, Congress should increase the Department of Defense's science and technology appropriations from 15.3% to 20% of the Department of Defense's overall RDT&E budget. Experts consider science and technology funding as "the pool of knowledge necessary for future military systems' development."[109] Every year, the allocation should be automatic without requiring the statutory research form submission that is part of the five-year planning, programming, budgeting, and execution process. The federal government should streamline its arduous and costly processes and return those savings to the federal government's budgets for disruptive innovation. By streamlining processes and automatically allocating additional science and technology funding, the U.S. government will accelerate the current process that falls years behind the speed of technology.[110] Investing in disruptive or transformative innovation will better prepare the United States to counter adversaries' threats.

Leverage shorter-term acquisition processes for distinct and embedded software and technology acquisition

Industry partners often comment that doing business with the government, especially in disruptive innovation and advanced computing, is too difficult. A higher percentage of the Department of Defense's budget must be allocated and appropriated by Congress outside the planning, programming, budgeting, and execution process to reduce the valley of death that prevents the operationalization of innovative technologies. The Department of Defense should use these additional resources to keep startup companies in cutting-edge technology alive.

Finally, Congress should eliminate unnecessary areas of the Federal Acquisition Regulation that over-emphasize documentation over capability delivery.

Incorporate increased automated accountability and reporting by employing big data analytics

Using artificial intelligence technology to access an ever-increasing quantity of data can improve the maintenance of deployed acquisitions and provide a successful measurement of policies, programs, and acquisitions. Improved data analytics will assist Department of Defense leadership in making data-driven decisions.

Incorporate flexible contracting vehicles to facilitate speed and agility

The government must encourage and employ versatile contracting approaches, including Blanket Purchase Agreements, Other Transaction Authorities, or Indefinite Delivery Indefinite Quantity contracts, to accelerate the time to procure and implement critical cybersecurity tools. Incorporating flexibility and agility into the U.S. acquisition process will provide solutions at the "speed of cyber" to counter these dynamic, persistent threats.

Centrally manage the licensing of crucial cyber enablers for the best value

The amount of information technology across the Department of Defense requires centralized procurement and management for all Program Executive Offices and Program Managers to reduce cost and improve cyber protection for the infrastructure. Control of this effort should be at the portfolio level aggregating acquisitions as much as possible. Software licenses such as Splunk and similar offerings are required to protect networks from intrusion (e.g., integrated solutions provided by Palo Alto). The U.S. government's contract with Microsoft provides one example of its efforts to secure cybersecurity software packages through centralized buys.

Augment training and collaboration between industry and government to improve intellectual property value

The Department of Defense should identify and continue to develop subject matter experts to advise Program Executive Officers and senior defense leaders on the importance of developing appropriate data rights agreements. The services will retain access to their data without paying contractors exorbitant fees for machine learning or other tools for which the data rights might not apply. This action will require extensive updates to the Defense Federal Acquisition Regulation Systems clauses. Avoiding unnecessary expenditures on this type of intellectual property will allow the U.S. government to allocate these scarce resources to beneficial cybersecurity or network protection.

Conclusion

The United States faces an increasingly complex array of threats to its national security, ranging from great economic and military power competitors, diverse non-traditional actors, emerging hybrid war tactics, cyberattacks, and disinformation campaigns. These threats lead many to question the world order, while others seek to steer the United States away from the democratic values it holds dear. In the face of rising international economic and security competition, compounded by emerging technologies, the United States must act now. These actions include establishing robust national cyber and innovation strategies, streamlining cyber coordination across the private, public, and international arenas, catalyzing innovation to ensure an edge in disruptive technology, and strengthening U.S. advanced computing supply chains. The United States must focus on the urgent and strategic need to revive innovation and entrepreneurship in strategic technologies – American values that have proven successful in times of great challenge to the United States. A whole-of-nation effort to spur innovation will increase U.S. economic and military strength and protect the homeland, values, and interests. The time is now to invest in the future and position the United States to continue shaping the future world order.

Appendix A – Organizations Interviewed

Figure 5. Collage of entities engaged during the Cybersecurity and Advanced Computing Industry Study during the NDU Eisenhower School Seminar 04 AY20-21. Logos from entities' webpages.

Appendix B – STEM Demographics

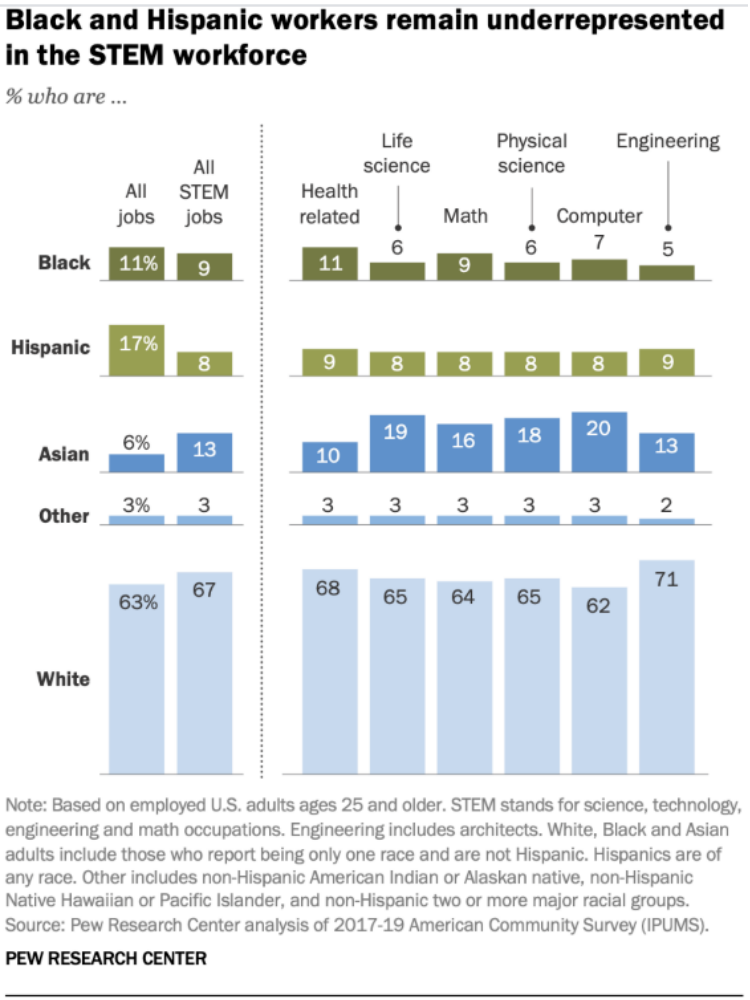

Figure 6. Illustration of underrepresentation of Black and Hispanic workers in the STEM workforce, from the Pew Research Center.

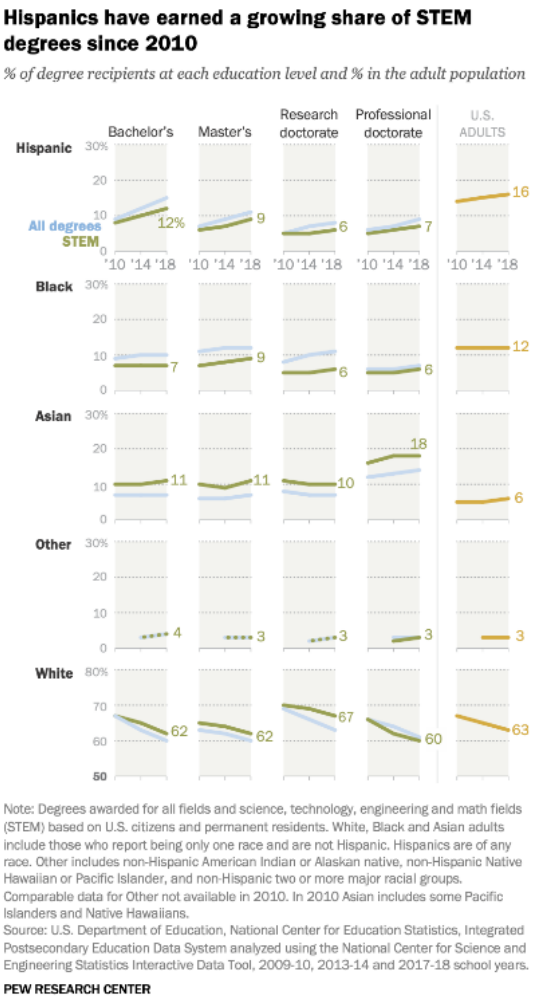

Figure 7. Illustration of Hispanics earning STEM degrees since 2010 by the Pew Research Center.

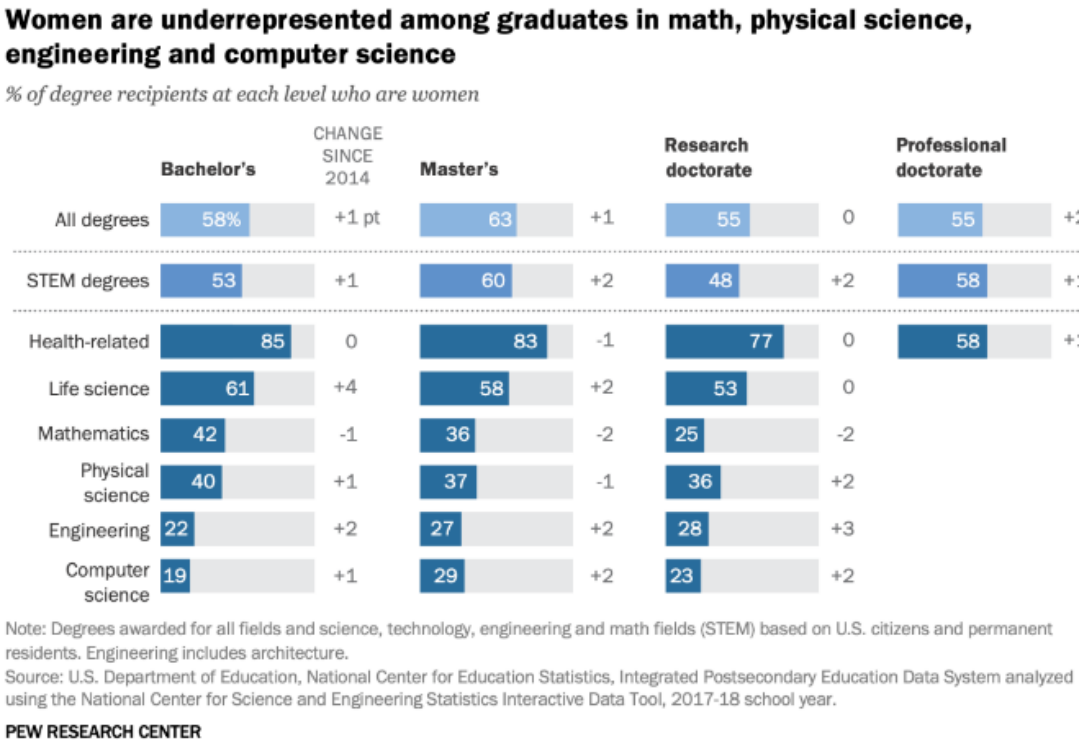

Figure 8. Illustration of the underrepresentation of women graduates in math, physical sciences, engineering, and computer science by the Pew Research Center.

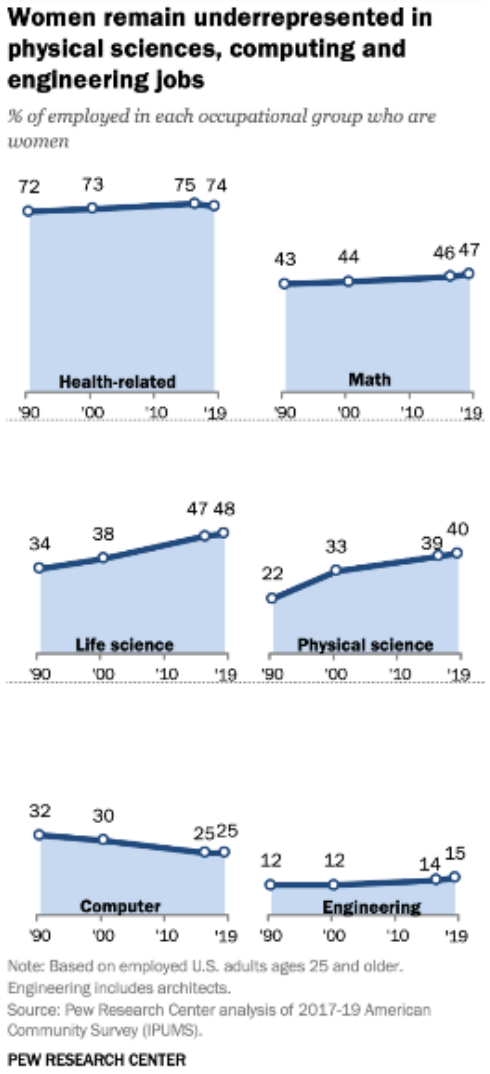

Figure 9. Illustration of underrepresentation of women in physical sciences, computing, and engineering jobs by the Pew Research Center.

Appendix C – Porter's Diamond Analysis

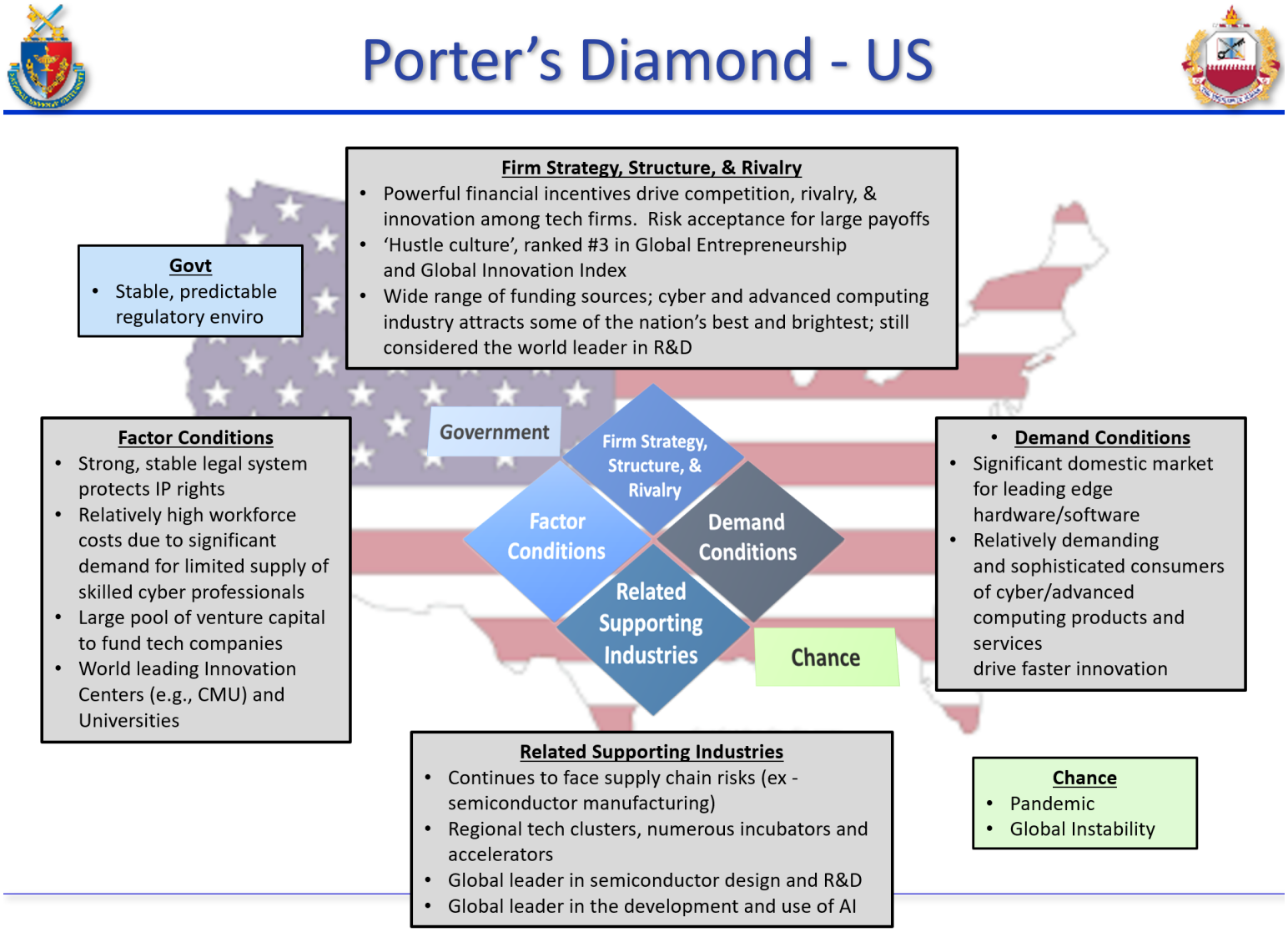

Figure 10. Porter's Diamond analysis of the United States by NDU Eisenhower School Seminar 04 AY20-21 (assessment based on multiple disparate sources).

Porter's Diamond - China

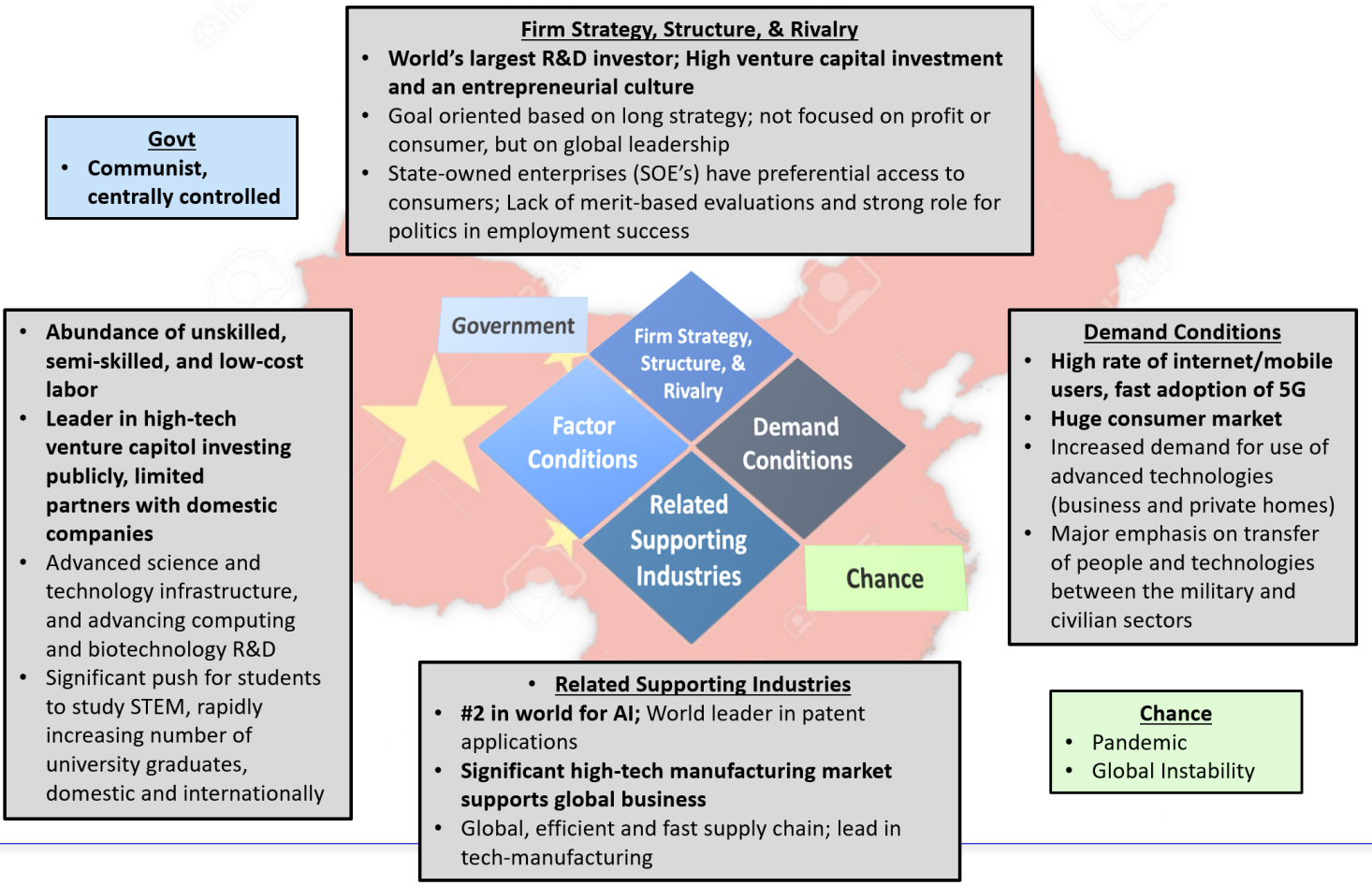

Figure 11. Porter's Diamond analysis of China by NDU Eisenhower School Seminar 04 AY20-21 (assessment based on multiple disparate sources).

Porter's Diamond - Taiwan

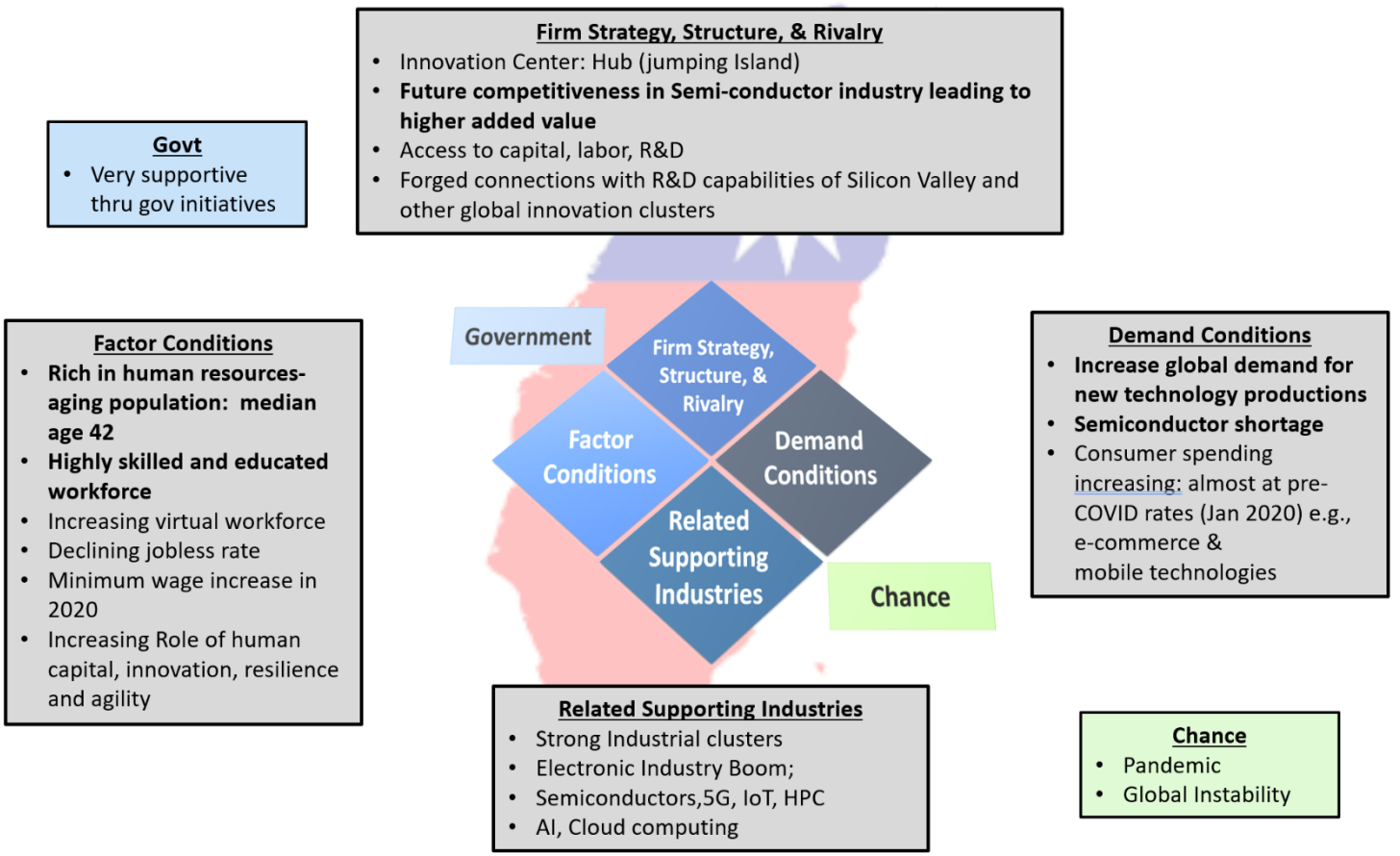

Figure 12. Porter's Diamond analysis of Taiwan by NDU Eisenhower School Seminar 04 AY20-21 (assessment based on multiple disparate sources).

Porter's Diamond - India

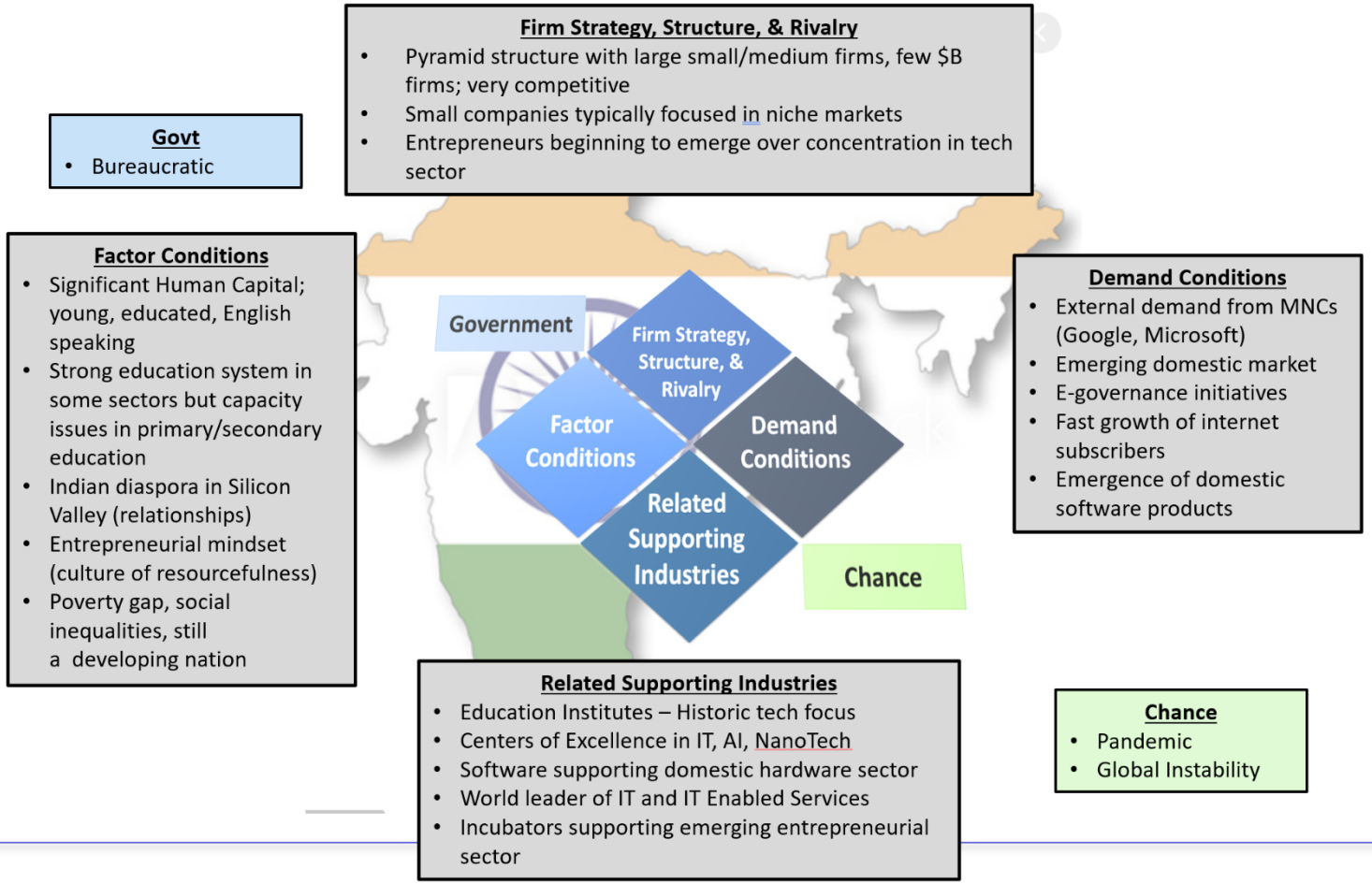

Figure 13. Porter's Diamond Analysis of India by NDU Eisenhower School Seminar 04 AY20-21 (assessment based on multiple disparate sources).

Porter's Diamond - Russia

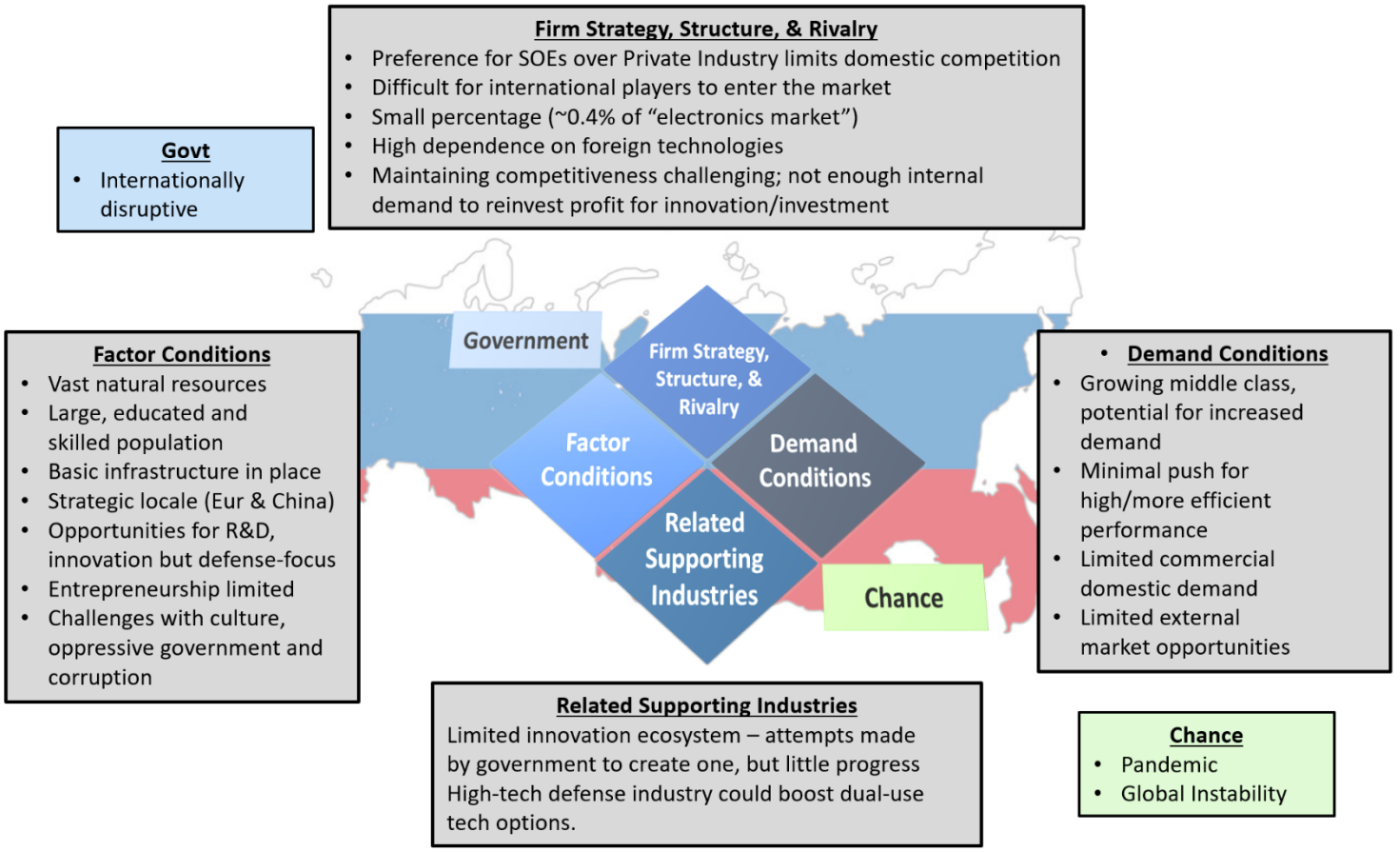

Figure 14. Porter's Diamond analysis of Russia by NDU Eisenhower School Seminar 04 AY20-21 (assessment based on multiple disparate sources).

Appendix D – Global 5G Telecommunication Suppliers

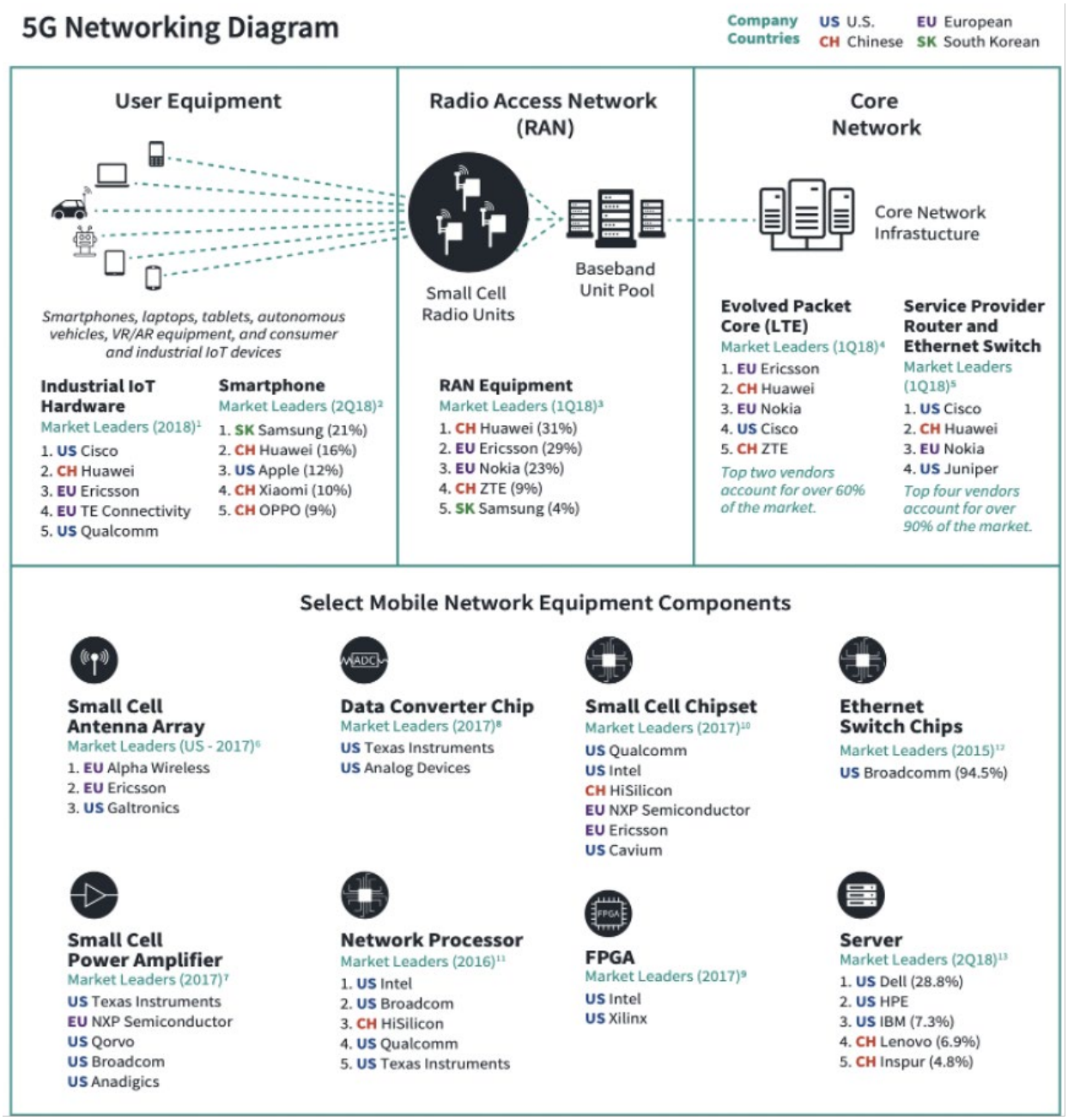

Figure 15. Illustration of 5G infrastructure suppliers by CSIS - How 5G Will Shape Innovation and Security: A Primer.[111]

Appendix E – Expanded Policy Recommendations

Develop an Innovation Task Force, Recommendations, and a Comprehensive Strategy

The first step toward developing a national strategy on innovation is establishing a task force that includes critical stakeholders who will review the landscape of strengths, weaknesses, opportunities, and threats and make recommendations for the U.S. government. Participants in this task force should include representatives from the National Security Council and all U.S. agencies involved in cyber and STEM. Given that much of the best U.S. innovation comes from the private sector, it will be essential to include companies driving innovation in strategic industries, including cyberspace and cybersecurity, telecommunications, health, space/air transportation, energy, and defense. Likewise, the task force should invite top leaders of innovation in academics and think tanks. Once the task force makes its recommendations and develops a national innovation strategy, the National Innovation Director should establish an ongoing consultative mechanism such as an advisory board. In structured meetings and open dialogue, the participants will have a venue to share ongoing challenges and identify opportunities for collaboration.

Target Assistance to Small and Medium Enterprises – Small Business Administration Programs

Small Business Innovation Research and Small Business Technology Transfer programs encourage small businesses to engage in federal R&D projects with the potential for commercialization. These initiatives can provide additional impetus to U.S. companies to establish and grow public-private partnerships. However, many budding technology companies have not gone public and therefore cannot qualify for these programs. The Small Business Administration should transform itself from a distant source of information only for fully functional businesses to a more interactive resource of practical assistance, especially for entrepreneurs and companies of strategic technologies, targeted communities, and underprivileged segments of society.

Promote STEM Careers – Space Force and Defense Outreach to Schools

There are many ways that the U.S. government should increase the visibility of government careers in space and STEM. The United States Space Force and renowned astronauts should launch a campaign highlighting careers in space and space technologies. Finally, the Department of Defense and the Armed Forces Communications and Electronics Association should implement the Tampa and Orlando, FL model. These Armed Forces Communications and Electronics Association chapters implemented a bright Army officer's vision to establish relationships with local high schools and colleges in STEM disciplines to enhance "the bridge between government requirements and industry capabilities."[112]

Update Immigration Laws Specific to Strategic Sectors
Overcoming Risks of Intellectual Property Espionage and Job Displacement

Resistance to policies designed to increase immigration includes the risks of intellectual property espionage and job displacement. A promising future in the United States could help

dissuade those students and workers in the United States in key sectors from engaging in commercial espionage and counter pressure by the Chinese Communist Party on its nationals in the United States. Bringing foreign talent into the U.S. workforce to build a new life here will provide much-needed skills in short supply. As to potential job displacement, a National Academy of Sciences report concludes that "immigration raises national output and on net improves the economic well-being of the native-born."[113]

Incorporate Innovation Best Practices
Diversity, Innovation Culture, and Improved Personnel Services.

A diverse workforce

The federal government must continue to develop a work environment that includes and respects differences, recognizes the unique contributions that diverse individuals can make, and maximizes the potential of all employees. Increased outreach to under-represented communities and improving hiring practices will help create diversity. Improved performance review and promotion policies and procedures will ensure government employees value diversity.[114]

Create a culture of innovation

The private sector, especially the technology industry, provides a work environment that promotes innovation and continued learning. The U.S. government should provide increased opportunities for virtual and in-person training classes, built into a career path plan for every employee. On-the-job training through coaching, feedback, and role modeling is another effective model for increasing job performance and satisfaction. The U.S. government could support increased external learning, such as tuition reimbursement programs and industry exchange programs, and subsidize advanced technical education programs and online technical certifications.

Streamline personnel systems, security clearances, and improve service

All military services should centralize personnel procedures for military and civilians into one cloud-based system to avoid duplicative entry and processes and better utilize the military's broad base of skills. Uniform standards across all government agencies and sufficient training of new investigative personnel should reduce the time needed for security clearances and more quickly fill needed positions. The U.S. government should streamline and improve human resource services, making information more readily accessible to serve U.S. government personnel better and develop and retain public talent.

Increase Funding for Science Agencies

On March 31, 2021, the White House announced its American Jobs Plan. The plan dedicates an unprecedented public investment of $100B in public schools, $12B in community colleges, $25B in minority-serving institutions (universities), $40B in dislocated working retraining, $12B in assistance for underserved workforce segments, $48B in apprenticeships, a $50B increase for the NSF, $30B for R&D in rural areas, $40B for R&D at national labs, and

$34B for innovation hubs.[115] However, compared to the over $2.2 trillion to be spent over ten years, the total $393B investment in U.S. education and STEM is disproportionately low (17.52%). This paper recommends dedicating a total of 20% (an increase of $55.6B) toward education and STEM-related R&D to ensure long-term U.S. competitiveness. The following table shows the investment in each category.

Table. American Jobs Plan Investments for 2021

Category	Allocation $B	% Total
Education	**237**	**10.6%**
Public Schools	100	4.46%
Community Colleges	12	0.53%
Minority Universities	25	1.11%
Dislocated Workforce Retraining	40	1.78%
Targeted Workforce Assistance	12	0.53%
Apprenticeships	48	2.14%
R&D	**154**	**6.9%**
National Science Foundation	50	2.23%
R&D to Rural Areas	30	1.34%
R&D National Labs	40	1.78%
Innovation Hubs and Technologies	34	1.52%
Manufacturing	**198**	**8.8%**
Domestic Manufacturers	52	2.32%
New Commerce Department Office	50	2.23%
Pandemics	40	1.78%
Clean Energy	46	2.06%
Workforce Protection	10	0.45%
Infrastructure	**832**	**37.1%**
Transportation	621	27.68%
Digital Infrastructure Policies	100	4.46%
Power Infrastructure	100	4.46%
Federal Buildings	11	0.49%
Quality of Life Improvements	**822**	**36.3%**
Combat Climate Change	50	2.23%
Clean water	111	4.95%
Housing	213	9.50%
VA Hospitals	18	0.80%
Rural Development	5	0.22%
Child Care	25	1.11%
Elderly & Disabled Care	400	17.83%
Total	**2,243**	

Source: Data from The White House, "Fact Sheet: The American Jobs Plan." Last modified March 31, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/

Notes

[1] Catherine A Theohary, *Defense Primer: Cyberspace Operations*, CRS Report No. IF10537 (Washington, DC: Congressional Research Service, 2020), https://crsreports.congress.gov/product/pdf/IF/IF10537.
[2] "Domain | Definition of Domain by Merriam-Webster," Merriam-Webster, accessed May 10, 2021, https://www.merriam-webster.com/dictionary/domain.
[3] "The SolarWinds Cyber-Attack: What You Need to Know," CIS, accessed May 13, 2021, https://www.cisecurity.org/solarwinds/; Jenni Bergal, "Florida Hack Exposes Danger to Water Systems," Pew, accessed May 13, 2021, https://pew.org/3btxWBc; "Multiple Vulnerabilities in Microsoft Exchange Server Could Allow for Arbitrary Code Execution," CIS, accessed May 13, 2021, https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-microsoft-exchange-server-could-allow-for-arbitrary-code-execution_2021-030/; Kevin Collier, "Colonial Pipeline Hack Claimed by Russian Group DarkSide Spurs Emergency Order from White House," NBC News, May 10, 2021, https://www.nbcnews.com/tech/security/colonial-pipeline-hack-claimed-russian-group-darkside-spurs-emergency-rcna878
[4] Wesley Chai, "What Is Telecommunications (Telecom)?," SearchNetworking, accessed March 20, 2021, https://searchnetworking.techtarget.com/definition/telecommunications-telecom.
[5] "Global IT Hardware," Industry Profile (MarketLine, May 2020), https://advantage-marketline-com.nduezproxy.idm.oclc.org/Analysis/ViewasPDF/global-it-hardware-101019.
[6] "Global Software," Industry Profile (MarketLine, February 2021), https://advantage-marketline-com.nduezproxy.idm.oclc.org/Analysis/ViewasPDF/global-software-122965.
[7] Will Kenton, "Human Capital," Investopedia, September 4, 2020, https://www.investopedia.com/terms/h/humancapital.asp.
[8] Sharon Anderson, "CHIPS Articles: Recruiting, Training and Maintaining Talent in the Cyber Workforce," *CHIPS The Department of the Navy's Information Techonology Magazine* July-September 2013 (n.d.), https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=4727.
[9] Nick Wadhams, "What Joe Biden Said About China in His First Speech to Joint Session of Congress - Bloomberg," Bloomberg, April 28, 2021, https://www.bloomberg.com/news/articles/2021-04-29/human-rights-defense-and-turbines-what-biden-said-about-china.
[10] Council of Europe, "Convention on Cybercrime" (Budapest, November 23, 2001), https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf; Eric Talbot Jensen, "The Tallinn Manual 2.0: Highlights and Insights," *Georgetown Journal of International Law* 48 (2017): 735–78.
[11] "Groups | MITRE ATT&CK®," MITRE, accessed May 1, 2021, https://attack.mitre.org/groups/; "Advanced Persistent Threat Groups (APT Groups) | FireEye," Fireeye, accessed April 28, 2021, https://www.fireeye.com/current-threats/apt-groups.html
[12] "Survey of Chinese-Linked Espionage in the United States Since 2000," Center for Strategic & International Studies, n.d., https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000.
[13] "Significant Cyber Incidents | Center for Strategic and International Studies," Center for Strategic & International Studies, accessed May 11, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
[14] "Advanced Persistent Threat Groups (APT Groups) | FireEye," Fireeye, accessed April 28, 2021, https://www.fireeye.com/current-threats/apt-groups.html.
[15] *Peter W. Singer on LikeWar: The Weaponization of Social Media*, 2019, https://www.youtube.com/watch?v=whBehefflQA.
[16] Sean Markey, "The Future of Democracy & Social Media," *Norwich Record*, accessed November 27, 2020, https://www.norwich.edu/record/2195-the-future-of-democracy-social-media.
[17] Markey, "The Future of Democracy & Social Media."; White House, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Washington, DC: White House, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.
[18] "Groups | MITRE ATT&CK®," MITRE, accessed May 1, 2021, https://attack.mitre.org/groups/.

[19] Jonathan Garber, "Iran-Linked Hackers Tried to Infiltrate Trump Campaign | Fox Business," Fox Business, October 9, 2019, https://www.foxbusiness.com/politics/iran-reportedly-tried-to-hack-at-least-one-presidential-candidate.
[20] Office of the Director of National Intellicece, "Annual Threat Assessment of the US Intelligence Community," April 9, 2021, 14, https://www.odni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
[21] Toi Staff, "Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps | The Times of Israel," Time of Israel, July 17, 2020, https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/.
[22] Proofpoint Threat Insight Team, "Threat Actor Profile: TA407, the Silent Librarian," Proofpoint, October 9, 2019, https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta407-silent-librarian.
[23] Proofpoint Threat Insight Team, "TA407, the Silent Librarian."
[24] "Groups | MITRE ATT&CK®," MITRE, accessed May 1, 2021, https://attack.mitre.org/groups/.
[25] Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies - Bloomberg," Bloomberg Businessweek, October 4, 2018, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.
[26] "These Countries Spend the Most on Research and Development," World Economic Forum, November 16, 2020, https://www.weforum.org/agenda/2020/11/countries-spending-research-development-gdp/.
[27] Niall McCarthy, "These Countries Spend the Most on University Research," World Economic Forum, November 5, 2019, https://www.weforum.org/agenda/2019/11/us-government-funded-university-research-slips-rankings/.
[28] John F. Sargent Jr, *Defense Primer: RDT&E*, CRS Report No. IF10553 (Washington, DC, 2020), https://crsreports.congress.gov/product/pdf/IF/IF10553; John F. Sargent, Jr., *Department of Defense Research, Development, Test, and Evaluation (RDT&E)*, CRS Report No. R44711 (Washington, DC: Congressional Research Service, 2020).
[29] Schaeffer, Chuck, "How Much Should You Invest in Innovation?" *Customer Think*, April 8, 2021, https://customerthink.com/how-much-should-you-invest-in-innovation/
[30] *National Security Commission on Artificial Intelligence Testimony Before the Senate Committee on Armed Services, Emerging Technologies and Defense: Getting the Fundamentals Right,* 117th Cong., 1st Session, February 23, 2021,
[31] Defense Innovation Unit, "About the Defense Innovation Unit," accessed April 28, 2021, DIU.
[32] Stephanie Meloni, "What the Defense Innovation Unit Wants Industry to Know About CSOs – Part 1." Immixgroup.com (blog). June 4, 2019. https://blog.immixgroup.com/2019/06/04/what-the-defense-innovation-unit-wants-industry-to-know-about-csos-part-1.
[33] Sarah Sybert, "Air Force Plans $1B ACT 3 Contract Vehicle For Cybersecurity Advancements - Executivebiz". Executivebiz, 2020. https://blog.executivebiz.com/2020/07/air-force-plans-1b-act-3-contract-vehicle-for-cybersecurity-advancements.
[34] Brian Kennedy, Richard Fry, and Cary Funk, "6 Facts about America's STEM Workforce and Those Training for It," *Pew Research Center* (blog), April 14, 2021, https://www.pewresearch.org/fact-tank/2021/04/14/6-facts-about-americas-stem-workforce-and-those-training-for-it/.
[35] "Code of Practice on Disinformation," *European Commission*, Accessed: May 12, 2021, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation; Levush, Ruth, "Government Responses to Disinformation on Social Media Platforms: Comparative Summary," *Library of Congress*, September 2019, https://www.loc.gov/law/help/social-media-disinformation/compsum.php
[36] "Global Cybersecurity Index," ITU, accessed April 26, 2021, https://www.itu.int:443/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[37] "Defense Industrial Base Sector," Critical Infrastructure Sectors, Cybersecurity and Infrastructure Secuirty Agency, accessed May 10, 2021, https://www.cisa.gov/defense-industrial-base-sector
[38] Angeli Datt and Sarah Cook, "The CCP is Retooling its Censorship System at a Brisk Pace in 2021," *China Brief* 21, iss. 8 (April 23, 2021): 14, https://jamestown.org/wp-content/uploads/2021/04/Read-the-4-23-2021-Issue-in-PDF.pdf?x43949
[39] White House, National Security Strategy of the United States of America (Washington, DC: White House, 2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
[40] President Barack Obama, *Presidential Policy Directive – United States Cyber Incident Coordination* (PPD-41), (Washington, DC: White House, 2016

[41] Joel Garverick, "Industry Study Lesson 7: Porter's Diamond and National Competitiveness" (Virtually National Defense University, Washington, DC, February 11, 2021), 4.
[42] Porter, Michael E., "The Competitive Advantage of Nations," *Harvard Business Review* 68, no 2 (March-April 1990): 77.
[43] Tim Zanni, "Technology Innovation Hubs," KPMG, 2020, 4, https://info.kpmg.us/content/dam/info/en/pdf/2020/tech-innovation-hubs.pdf.
[44] Michael E. Porter, "The Competitive Advantage of Nations," *Harvard Business Review*, March-April 1990, 73, http://www.economie.ens.fr/IMG/pdf/porter_1990_-_the_competitive_advantage_of_nations.pdf.
[45] Porter, Competitive Advantage of Nations, 77.
[46] David A. Powner, *CYBERSPACE: United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, DC: Government Accountability Office, 2010), https://www.gao.gov/products/gao-10-606
[47] Nick Marinos et al., *HIGH RISK SERIES: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, GAO-21-288 (Washington, DC: Government Accountability Office, 2021), 15-16, https://www.gao.gov/assets/gao-21-288.pdf
[48] Ross Garnaut, Ligang Song, and Cai Fang, "China's 40 Years of Reform and Development 1978-2018," *Australian National University Press*, 2018, http://www.iberchina.org/files/2019/40_years_refom_china_anu.pdf.
[49] Congressional Research Service, "U.S.-China Investment Ties: Overview," January 15, 2021, https://fas.org/sgp/crs/row/IF11283.pdf; James Andrew Lewis, "Technological Competition and China," *Center for Strategic & International Studies*, November 30, 2018, https://www.csis.org/analysis/technological-competition-and-china
[50] Ross Garnaut, Ligang Song, and Cai Fang, "China's 40 Years of Reform and Development 1978-2018," *Australian National University Press*, 2018, http://www.iberchina.org/files/2019/40_years_refom_china_anu.pdf.
[51] James L. Schoff and Asei Ito, "Competing With China on Technology and Innovation," Alliance Policy Coordination Brief, *Carnegie Endowment for International Peace*, October 2019, https://carnegieendowment.org/files/ChinaRiskOpportunity-China_Tech.pdf.
[52] Joseph Kannarkat and Norman Augustine, "One Lesson the U.S. Can Learn From China to Improve its Competitiveness in Technology Development," *Brooking Techtank*, January 19, 2021, https://www.brookings.edu/blog/techtank/2021/01/19/one-lesson-the-u-s-can-learn-from-china-to-improve-its-competitiveness-in-technology-development.
[53] Frank Tang, "China Pledges Greater Protection for Hi-tech Intellectual Property," *South China Morning Post*, April 25, 2021, https://www.scmp.com/news/china/politics/article/3131007/china-pledges-greater-protection-hi-tech-intellectual-property; Arjun Kharpal, "In a Quest to Rein In Its Tech Giants, China Turns to Data Protection," *CNBC*, April 11, 2021, https://www.cnbc.com/2021/04/12/china-data-protection-laws-aim-to-help-rein-in-countrys-tech-giants.html.
[54] Kharpal, "China Turns to Data Protection."
[55] Remco Zwetsloot and Dahlia Peterson, "The US-China Tech Wars: China's Immigration Disadvantage – How the United States Can Retain Technological Leadership Despite Its Demographic Deficit," *The Diplomat*, December 31, 2019, https://thediplomat.com/2019/12/the-us-china-tech-wars-chinas-immigration-disadvantage.
[56] Fainshmidt, Stav, Adam Smith, and William Q. Judge. "National Competitiveness and Porter's Diamond Model: The Role of MNE Penetration and Governance Quality." *Global Strategy Journal* 6, no. 2 (May 2016): 87. Accessed May 17, 2021 http://eds.a.ebscohost.com.nduezproxy.idm.oclc.org/eds/pdfviewer/pdfviewer?vid=2&sid=4ee8d468-7f3f-46ba-99b4-096d4fba31f5%40sessionmgr4007.
[57] Weiss, Andrew S., "New Tools, Old Tricks: Emerging Technologies and Russia's Global Tool Kit," *Carnegie Endowment for International Peace*, April 29, 2021, Accessed May 17, 2021 https://carnegieendowment.org/2021/04/29/new-tools-old-tricks-emerging-technologies-and-russia-s-global-tool-kit-pub-84437.
[58] Weiss, "New Tools, Old Tricks."
[59] Weiss, "New Tools, Old Tricks."
[60] Weiss, "New Tools, Old Tricks."
[61] Industrial Development Bureau, Taiwan Ministry Of Economic Affairs, "Important Policies" Moeaidb.Gov.Tw, 2021, https://www.moeaidb.gov.tw/ctlr?lang=1&PRO=english.rwdAbout02.

[62] "Science And Technology Competitiveness Rankings", Moea.Gov.Tw, 2021, https://www.moea.gov.tw/MNS/doit_e/content/Content.aspx?menu_id=20964.
[63] Industrial Development Bureau, Taiwan Ministry Of Economic Affairs, "Important Policies"
[64] Industrial Development Bureau, Taiwan Ministry Of Economic Affairs, "Important Policies"
[65] Industrial Development Bureau, Taiwan Ministry Of Economic Affairs, "Important Policies"
[66] "Taiwan Economy: Population, GDP, Inflation, Business, Trade, FDI, Corruption", Heritage.Org, 2021, https://www.heritage.org/index/country/taiwan.
[67] Evan Feigenbaum, "Assuring Taiwan's Innovation Future", Carnegie Endowment For International Peace, 2020, https://carnegieendowment.org/2020/01/29/assuring-taiwan-s-innovation-future-pub-80920.
[68] Feigenbaum, "Assuring Taiwan's Innovation Future."
[69] Sankalpa Bhattacharjee and Debkumar Chakrabarti, "Investigating India's Competitive Edge in the IT-ITeS Sector," *IIMB Management Review* (2015) 27: 19-34.
[70] "IT & BPM Industry in India," India Brand Equity Foundation, May 7, 2021, https://www.ibef.org/industry/information-technology-india.aspx.
[71] "India to Become 5th Largest Economy in 2025, 3rd Largest by 2030," *The Economic Times*, December 26, 2020, https://economictimes.indiatimes.com/news/economy/indicators/india-to-become-5th-largest-economy-in-2025-3rd-largest-by-2030/articleshow/79964750.cms?from=mdr.
[72] Bhattacharjee and Chakrabarti, "Investigating India's Competitive Edge," 22.
[73] Noshir Kaka, Anu Madgavkar, Alok Kshirsager, Rajat Gupta, James Manyika, Kushe Bahl, and Shishir Gupta, *Digitial India: Technology to Transform a Connected Nation*, McKinsey Global Institute, (New York: McKinsey Institute, 2019), https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.
[74] "Education System Profiles – Education in India," World Education News + Reviews, September 13, 2018, https://wenr.wes.org/2018/09/education-in-india.
[75] "Make in India," National Investment Promotion and Facilitation Agency, accessed on May 9, 2021, https://www.makeinindia.com; Kaka et al., *Digital India.*
[76] Kiesha Frue, "SWOT Analysis of India," Pestle Analysis, April 29, 2019, https://pestleanalysis.com/swot-analysis-of-india/; Elena Glibart, "SWOT Analysis of Indian IT Industry: Strengths," Mindstick, July 8, 2016, https://www.mindstick.com/articles/12169/swot-analysis-of-indian-it-industry-strengths.
[77] Lionel Sujay Valishery, "IoT connected devices worldwide 2030," Statista, January 22, 2021, https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/
[78] Valishery, "IoT connected devices worldwide 2030."/
[79] Marissa Norris, "Quantum Computers Will Break the Internet, but Only If We Let Them," April 9, 2020, https://www.rand.org/blog/articles/2020/04/quantum-computers-will-break-the-internet-but-only-if-we-let-them.html.
[80] Gwyneth Iredale, "Top Disadvantages of Blockchain Technology," 101 Blockchains, April 17, 2020, https://101blockchains.com/disadvantages-of-blockchain/
[81] Trevor Logan and Theo Lebryk, "America and its military need a blockchain strategy," C4ISRNET, April 5, 2021, https://www.reuters.com/world/china/biden-welcome-japans-suga-first-guest-key-ally-china-strategy-2021-04-16/
[82] Logan and Lebryk, "America"
[83] Logan and Lebryk, "America"
[84] Naveen Goud, "Microsoft acquires CyberX for $180 million," Cybersecurity Insiders, Accessed May 10, 2021, https://www.cybersecurity-insiders.com/microsoft-acquires-cyberx-for-180-million/
[85] Value Technology Foundation, "Potential Uses of Blockchain by the U.S. Department of Defense," Value Technology Foundation, March 2020, 5, https://www.crowell.com/files/Potential-Uses-of-Blockchain-Technology-In-DOD.pdf
[86] Value Technology Foundation, "Potential Uses," 34
[87] The White House, "Interim National Security Strategic Guidance" (Washington, DC: The White House, 2021), https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf.
[88] Stephen Nellis, "Phoenix Okays Development Deal with TSMC for $12 Billion Chip Factory," *Reuters*, November 18, 2020, https://www.reuters.com/article/us-tsmc-arizona/phoenix-okays-development-deal-with-tsmc-for-12-billion-chip-factory-idUSKBN27Y30E.

[89] Sarah Ravi, "Growth-Based Incentives, Not Tariffs, Will Strengthen U.S. Chip Manufacturing and Leadership," *Semiconductor Industry Association* (blog), July 2, 2020, https://www.semiconductors.org/growth-based-incentives-not-tariffs-will-strengthen-u-s-chip-manufacturing-and-leadership/.
[90] The Semiconductor Industry Association (SIA), "Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain" *(March 15, 2021) Submitted April 5, 2021,* https://www.semiconductors.org/wp-content/uploads/2021/04/4.5.21-SIA-supply-chain-submission.pdf.
[91] The Semiconductor Industry Association (SIA), "Risks in the Semiconductor Manufacturing and Advanced Packaging Supply Chain"
[92] Semiconductor Industry Association (SIA), "Semiconductors & the World Trade Organization," November 2020, https://www.semiconductors.org/wp-content/uploads/2020/11/The-WTO-and-the-Semiconductor-Industry-Nov-20201.pdf.
[93] Miller, James N. and Robert Butler, "Making the National Cyber Director Operational With a National Cyber Defense Center," *LawFareBlog*, March 24, 2021, https://www.lawfareblog.com/making-national-cyber-director-operational-national-cyber-defense-center
[94] Value Technology Foundation, "Potential Uses," 34
[95] Defense Science and Technology: Adopting Best Practices Can Improve Innovation Investments and Management, *Government Accountability Office*, Washington DC: Government Printing Office, June 2017, https://www.gao.gov/assets/690/685524.pdf
[96] McKinnon, John D., "Biden Addresses Global Competition on Technology: 'We're Falling Behind'," *The Wall Street Journal*, April 28, 2021, https://www.wsj.com/livecoverage/biden-speech-tax-antipoverty-plan-congress/card/4bUsQ99skksrOADCy4Jr
[97] The White House, "Interim National Security Strategic Guidance," *Whitehouse.gov*, March 2021, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
[98] Muro, Mark and Bruce Katz, "The New 'Cluster Moment': How Regional Innovation Clusters Can Foster the Next Economy," *Brookings Institution: Metropolitan Policy Program*, September 2010, https://www.brookings.edu/wp-content/uploads/2016/06/0921_clusters_muro_katz.pdf
[99] Lauckner, Sally, "How Many Small Businesses Are in the U.S.? (And Other Employment Stats)," *Fundera*, September 9, 2020, www.fundera.com/blog/small-business-employment-and-growth-statistics
[100] "CCDCOE to Host the Tallinn Manual 3.0 Process," *CCDCOE.org*, Accessed: May 12, 2021, https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/
[101] The White House, "Fact Sheet: The American Jobs Plan," *WhiteHouse.gov | Briefing Room*, March 31, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/
[102] "Common App," Accessed: February 28, 2021, https://www.commonapp.org/; "American Council on Education," Accessed: February 28, 2021, https://www.acenet.edu/Pages/default.aspx; "IIE: The Power of International Education," *IIE*, Accessed: February 28, 2021, https://www.iie.org/
[103] "Standards in Your State," *Common Core State Standards Initiative*, http://www.corestandards.org/standards-in-your-state/
[104] "About Achieve," *Achieve.org*, Accessed: April 10, 2021, https://www.achieve.org/about-us; "Improving Science Education Through Three-Dimensional Learning," *Next Generational Science Standards*, Accessed: April 10, 2021, https://www.nextgenscience.org/.
[105] Roberts, Joe, "Arts Entrepreneurship: Education, Theory, and Practice," Accessed: February 27, 2021, https://oxfordre.com/business/view/10.1093/acrefore/9780190224851.001.0001/acrefore-9780190224851-e-100
[106] The White House, "Fact Sheet: President Biden Sends Immigration Bill to Congress as Part of His Commitment to Modernize our Immigration System," *WhiteHouse.gov*, January 20, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/01/20/fact-sheet-president-biden-sends-immigration-bill-to-congress-as-part-of-his-commitment-to-modernize-our-immigration-system/; "Biden Administration Introduces 'U.S. Citizenship Act' Immigration Bill in Congress," *JDSUPRA*, February 22, 2021, https://www.jdsupra.com/legalnews/biden-administration-introduces-u-s-9426743/
[107] The White House, "Executive Order on America's Supply Chains," *WhiteHouse.gov*, February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
[108] Schaeffer, Chuck, "How Much Should You Invest in Innovation?" *Customer Think*, April 8, 2021, https://customerthink.com/how-much-should-you-invest-in-innovation/

[109] John F. Sargent, Jr., *Department of Defense Research, Development, Test, and Evaluation (RDT&E)*, CRS Report No. R44711 (Washington, DC: Congressional Research Service, 2020), https://crsreports.congress.gov/product/pdf/R/R44711.
[110] Power, Brad and Steve Stanton, "How to Prioritize Your Innovation Budget," *Harvard Business Review*, September 24, 2014, https://hbr.org/2014/09/how-to-prioritize-your-innovation-budget?registration=success
[111] Source: CSIS: How 5G Will Shape Innovation and Security: A Primer
[112] Military Leader, Class Notes for Cyber Industrial Study, National Defense University, Ft. McNair, VA, 20319.
[113] Smith, James P., and Barry Edmonston. The New Americans: Economic, Demographic, and Fiscal Effects of Immigration. Washington, DC: *National Academy Press*, 1997, pg. 142, 146, https://doi.org/10.17226/5779
[114] Harmeling, Susan S. and Charles M. Henderson, "Viewpoint: How Biden Can Foster a More Inclusive America," *Government Executive*, February 2, 2021, https://www.govexec.com/management/2021/02/viewpoint-how-biden-can-foster-more-inclusive-america/171799/
[115] The White House, "Fact Sheet: The American Jobs Plan," *WhiteHouse.gov | Briefing Room*, March 31, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/