WHY U.S. NATIONAL SECURITY REQUIRES A ROBUST, INNOVATIVE TECHNOLOGY SECTOR

Loren B. Thompson, Ph.D.

Lexington Institute

October 2020

Summary Contents

Introduction: America is facing the most serious challenge to its security in a generation……..page 3

What is the technology sector, and why will it be central to national security in the years ahead?.....page 4

What are the key trends in new technology likely to shape U.S. power militarily, economically and culturally?……..page 6

America's military has bold plans for using new technology to stay ahead of foreign rivals……....page 8

Other countries are working hard to match and surpass the United States in cutting-edge technologies……...page 11

China and Russia employ cyberattacks and other illegal means to steal U.S. intellectual property…….page 13

Cybersecurity is an indispensable feature of the nation's technology sector……...page 16

Conclusion: The United States will lose its status as the world's leading economic and military power if its technology sector falters……....page 18

Introduction: America is facing the most serious challenge to its security in a generation.

Every nation strives for security. Although the phrase "national security" in common usage has military overtones, there are other elements as well—economic, demographic, cultural. For instance, energy security was a major concern of U.S. policymakers in recent decades, and environmental security related to climate change now garners similar interest.

What every facet of national security has in common, though, is that it is shaped by technology. The wide oceans separating North America from the Eurasian land mass were once thought to confer military security on the republic, but long-range weapons altered the significance of distance. The rapid rise of formerly poor East Asian nations has been driven in large part by their mastery of technologies that did not exist two generations ago.

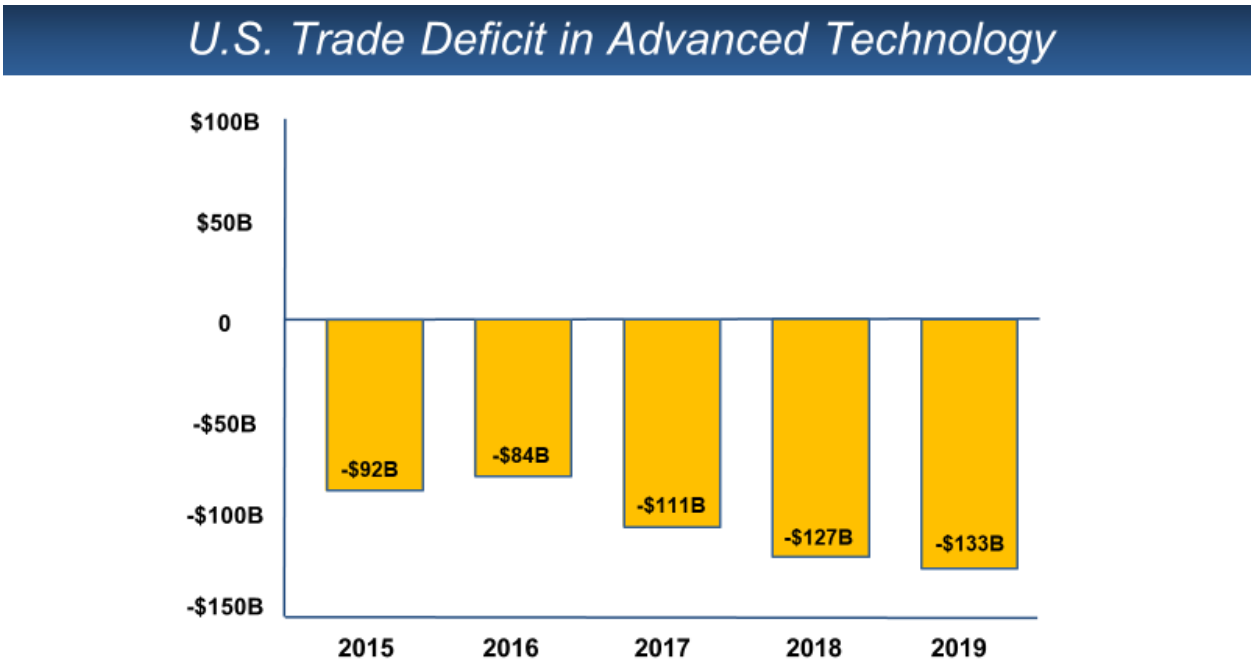
Technology is thus a critical driver of national security, because it is the variable that determines the significance of all the other factors. In the past, the United States was able to sustain a culture of innovation that permitted it to lead the world in advanced technologies. Now that may be changing as other nations pursue investment initiatives aimed at dominating the global information revolution. For example, the Chinese economy today generates as much manufactured output as Germany, Japan and America combined, and that output increasingly consists of advanced information technology.

This report is about the role that America's own technology sector plays in bolstering national security. It is focused mainly on the defense dimensions of America's strategic competition with China and other nations, illuminating how a robust and innovative domestic technology sector can contribute directly and indirectly to U.S. military dominance.

The United States has faced major challenges to its military security in every generation since the 20th century began, and in each case new technology was a key factor defining the danger. The threat posed by imperialism at the century's beginning was closely associated with

development of the dreadnaught. The threat posed by fascism a generation later was driven largely by the advent of air power. And the threat posed by communism in the century's second half arose first and foremost from nuclear weapons.

Unlike those earlier dangers, the technological content of today's threat from other nations is grounded largely in commercial innovations—innovations readily adapted to new concepts of warfare. If the United States is to emerge from this latest contest with its leadership position intact, as it did in earlier rivalries, it will have to compete successfully in commercial markets through commercial enterprises. This is not an "arms race" in the traditional sense, but its implications for America's place in the world are every bit as serious as the danger posed by dreadnaughts and bombers in earlier generations.



What is the technology sector, and why will it be central to national security in the years ahead?

The domestic technology sector is that part of the national economy devoted to developing and exploiting new information technologies. During the 1960s and 1970s, it was defined by information hardware such

as mainframe computers and semiconductors. The definition later expanded to include enterprises focused on the generation of software. More recently, it has come to encompass companies whose business lines are enabled by the internet, such as Google and Facebook.

It is not easy to define the boundaries of the technology sector, because every segment of the economy now relies on digital innovations and the internet to function. Hardware such as the smartphone is central to the emerging information economy, but many tech companies are engaged primarily in delivering services leveraged off of that hardware. For example, Amazon has transformed marketing and logistics using an internet-based business model, but it is mainly a provider of services rather than hardware. It is, nonetheless, a technology-driven change agent that is revolutionizing commerce.

The military's interest in the technology sector arises from the fungibility of information innovations across all facets of human activity. The same processors and memory chips that enable iPhones can be applied to smart weapons, battlefield communications, and military training devices. The same algorithms that facilitate machine learning in commercial products can be used to operate unmanned attack drones and autonomous fighting vehicles. And the "internet of things" that links disparate appliances is a model for the joint connectivity the military seeks in wartime.

There is a broad consensus among military planners that the industrial model of warfare spawned by 20th century conflicts is giving way to an information-driven model enabled by new digital technologies. Collectively, these technologies allow warfighters to find, fix and defeat threats faster than adversaries can, while minimizing dangers arising from the fog of war such as fratricide. But the process of innovation is unfolding at a furious pace, and America's military is hard-pressed to keep up. In August of 2020, the chief of staff of the Air Force released a strategy document aptly titled *Accelerate Change Or Lose.*

The fear among military planners is that a near-peer adversary might use new technologies to leapfrog beyond the warfighting capabilities of

America's joint force, exploiting technologies that barely existed when the current force was conceived. In June of 2020, the Pentagon's director of research and engineering issued a list of the highest-priority technologies in which the military needed to invest. The top technologies, in descending order of importance, were (1) microelectronics, (2) 5G communications, (3) hypersonics, (4) biotechnology, (5) artificial intelligence, (6) autonomy, and (7) cyber technologies. Only one of these technologies is predominantly military in character; all the others are mainly the products of commercial innovation.

They are also all technologies that China and other nations have disclosed plans to invest in heavily as they strive to overtake the United States. So from a military perspective, the threat posed by new information technologies is twofold. On the one hand, the United States might be overtaken and surpassed in operationalizing the new technologies as tools for gaining military advantage in future conflicts. On the other hand, if America cannot keep up in the race to innovate, it might eventually lack the economic resources needed to sustain a global military posture.

The U.S. government, and the Department of Defense in particular, invests extensively in such technologies. However, it is widely recognized that the private sector is where innovation in advanced technologies occurs more quickly and more imaginatively. Government can help industry to innovate with targeted funding, tax policy and other exertions, but it cannot create a culture of innovation within the public sector. That requires a structure of incentives that exists only in the marketplace.

What are the key trends in new technology likely to shape U.S. power militarily, economically, and culturally?

New technology has been reshaping civilization at an increasingly rapid pace since the beginning of the industrial revolution. The United States became an independent nation as that revolution was beginning, and thus has been a beneficiary of the innovations that followed. Because it fostered a uniquely open and rewarding setting for inventors such as Edison and

Ford, America was able to ride the wave of innovation unfolding in the 19th and 20th centuries to become the most powerful nation in history.

Whether the United States continues to enjoy that status in the current generation will depend on its ability to lead the information revolution currently transforming global commerce and culture. Most of the world's leading technology companies are headquartered in America, and the innovations they generate have spread rapidly to every corner of the planet. For example, Google's Android operating system is the global standard for smartphones, and over three billion people use Facebook services.

Numerous experts have speculated about which technologies will prove most decisive in determining who will win or lose in the years ahead. The innovations most frequently cited are artificial intelligence and machine learning, genomics and gene editing, 5G communications, the "internet of things," big data analytics, robotics and autonomous vehicle technology, and cybersecurity. Any one of these innovations could have a greater impact than the others, but because all are in their infancy it is impossible to know at present which will be most important.

However, it is not too soon to say what the key innovations have in common. They all depend on microelectronics and increasingly agile source code. They all utilize the internet to share ideas and information. They all tend toward open architectures and modular designs that can be easily modified. And because they are all relatively new, their full potential has yet to be realized. The latter point implies that the future of civilization is promising but unpredictable. For instance, modification of the human genome using information tools has already begun, with unknowable long-term consequences for civilization.

Although the United States continues to lead the world in basic research on new information technologies, it is gradually losing its edge in the manufacture of cutting-edge innovations. That applies not just to the production of hardware such as flat-screen displays and smartphones, but also the production of pharmaceuticals and other technology-intensive

commodities. This trend results from myriad causes—tax policy, labor costs, trade practices, government regulations—but it has been unfolding for decades and potentially impairs the capacity of America to stay ahead. The Pentagon has repeatedly warned that growing reliance on offshore sources for production of new technologies is a threat to U.S. security.

Another important trend that has appeared as domestic manufacturing declined is that the most innovative technology companies have increasingly focused on services as their primary product. Google, the originator of Android and operator of the world's most ubiquitous search engine, is an obvious example of this trend, as are Facebook and Amazon. The shift to services is reflected in the fact that the U.S. has large trade deficits in advanced technology hardware, but a robust trade surplus in services.

It is not clear whether the offshoring of technology production and shift to services will profoundly impact the global position of the United States—most of the value added in iPhones still originates domestically in the form of software and applications—but the recent pandemic has demonstrated the dangers of being excessively dependent on foreign sources for vital supplies. As federal policy changes to promote revitalization of domestic manufacturing, information technologies will play an important role in creating world-class production facilities. This is yet another way in which the technology sector is critical to American power and prosperity.

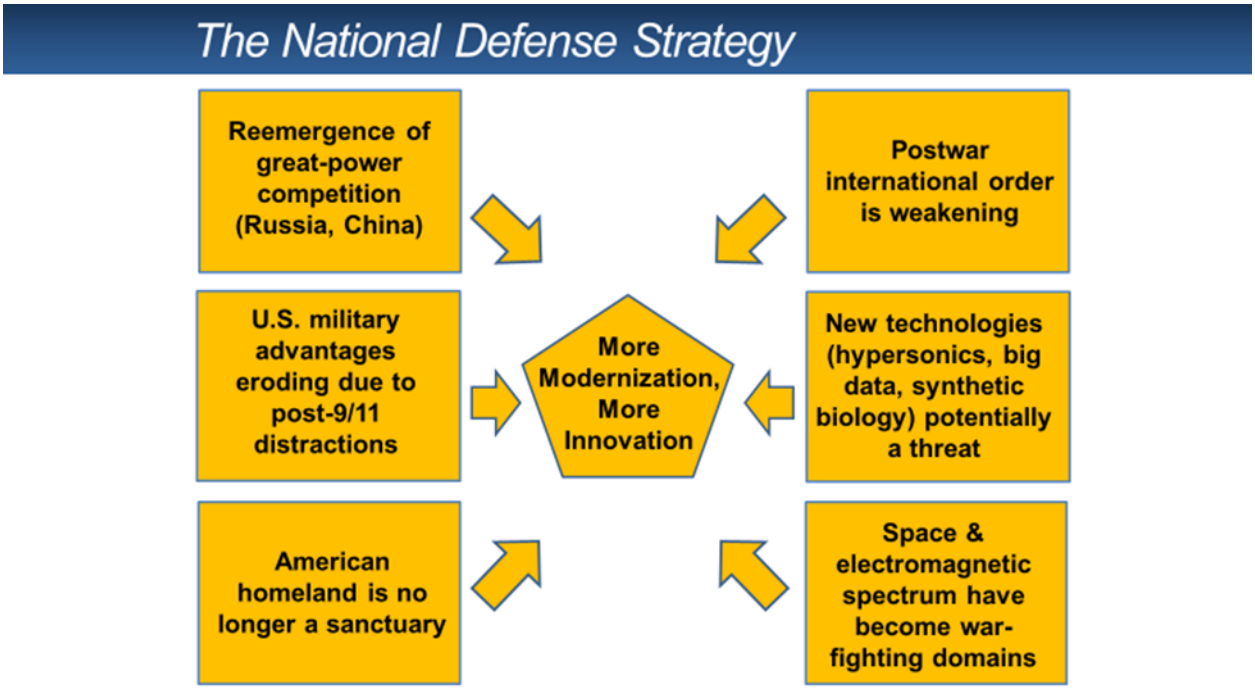
America's military has bold plans for using new technology to stay ahead of foreign rivals.

In May of 2000, the Joint Chiefs of Staff released a document entitled *Joint Vision 2020* that summarized U.S. military plans for staying ahead of overseas adversaries. The document emphasized the importance of technological innovation, stating that "the ongoing 'information revolution' is creating not only a quantitative, but a qualitative change in the information environment that by 2020 will result in profound changes

in the conduct of military operations." This proved to be one of the most prescient predictions in Pentagon history.

The global war on terror provided experience in applying new technologies to elusive threats, producing numerous innovations in sensing, targeting and force coordination. By the second decade of the new century, though, it was becoming apparent that the future threat environment would be dominated not by irregular forces, but by near-peer military powers such as China and Russia. The Obama Administration developed a "third offset strategy" aimed at leveraging emerging technology to stay ahead of near peers.

The Trump Administration's 2018 National Defense Strategy confirmed the return to a focus on great-power rivalry, with a principal focus on deterring and/or defeating the rising power of China. New technologies figured prominently in the defense strategy's description of both the threat and the appropriate response. A sample of Pentagon investment initiatives demonstrates how central new technology, especially commercial technology, is to the nation's military strategy.



Multi-domain operations. Each of the armed forces has traditionally focused on a specific domain of warfare, with the Navy emphasizing maritime operations, the Army stressing land operations, and the Air Force absorbed in airborne operations. The new paradigm of national defense adds conflict in space and on the electromagnetic spectrum to the traditional warfighting domains, and directs each of the services to prepare for operations across all five domains. That goal is impossible to accomplish without applying an array of information technologies to the tasks of securely communicating and managing operations across service lines in a dynamic combat environment.

Autonomous combat systems. Each of the military services is developing unmanned vehicles capable of operating for extended periods in the fog of war, thereby reducing the risk to U.S. warfighters. For instance, the Air Force has awarded contracts for a robotic wingman called Skyborg that would supplement or replace manned aircraft operating in heavily contested air space. The Navy is developing a family of surface and undersea warships that can operate autonomously for a month or longer. These programs depend heavily on machine learning and other fruits of the information revolution to function.

Responsive logistics. Military supply operations historically have been characterized by extensive waste and inability to deliver critical items to intended users on a timely basis. By applying big data analytics, GPS tracking and digital networking to the logistics function, the joint force is finding ways of making the supply function faster and better tailored to the precise needs of warfighters. Many of the innovations being used originated in the commercial technology sector and continue to be predominantly commercial in character.

Dozens of such initiatives are being pursued across the joint force, leveraging such information-driven advances as digital engineering and rapid software development. Cybersecurity is also a pervasive requirement, because all of the information technologies being adapted to military use from chips to links to software can potentially be compromised by intruders if they are not properly protected.

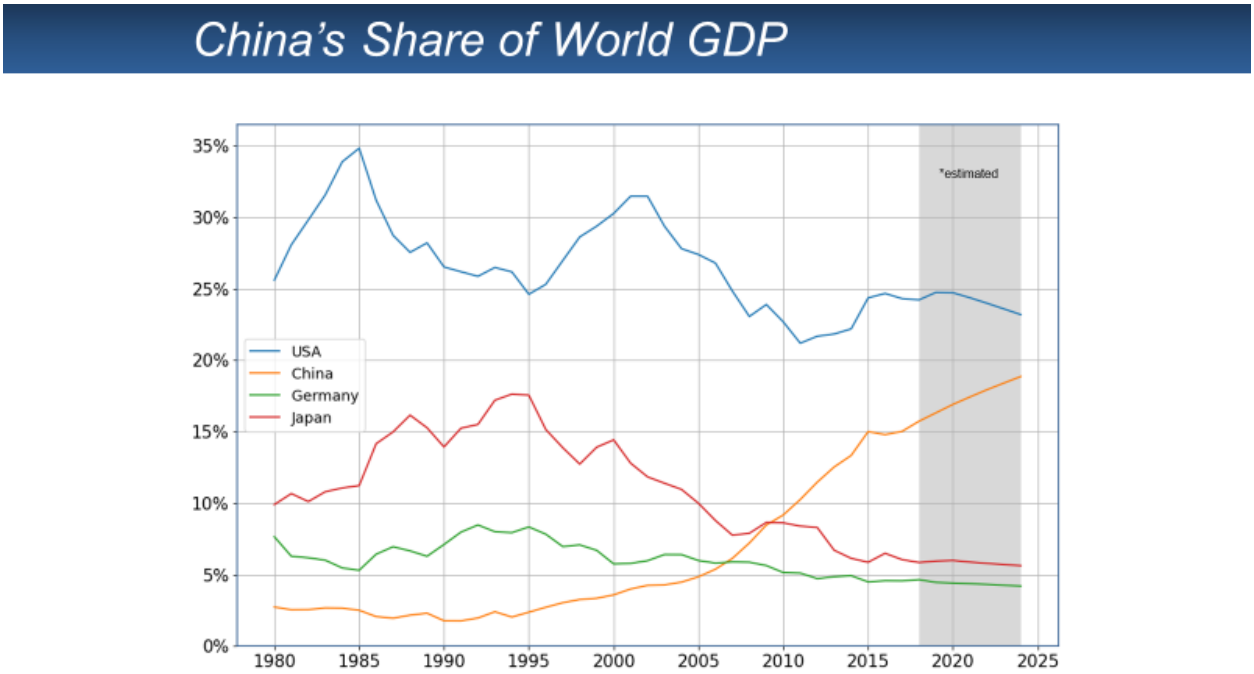
Other countries are working hard to match and surpass the United States in cutting-edge technologies.

China is following the same path that other Asian countries such as Japan and South Korea previously did in trying to modernize their economies, albeit on a far grander scale. Rather than adhering to the free-trade, open-market principles championed by Western nations, Beijing has embraced an aggressive form of mercantilism that includes tariffs, subsidies, forced technology transfers and other protectionist elements aimed at rapidly building up key industries. Many of these measures are incompatible with commitments the Chinese government made when it joined the World Trade Organization in 2001.

In 2015, Beijing launched a ten-year plan called "Made In China 2025" aimed at becoming proficient in ten key industries that the U.S. Council on Foreign Relations has described as an "existential threat to U.S. technological leadership." The ten industries include information technologies, robotics, aerospace, pharmaceuticals, electric vehicles and advanced materials. The goal is for domestic sources to provide 40% of content in these critical industries by 2020, and 70% by 2025. Over the longer term, China seeks to gain control of global supply chains for advanced industries, and displace the United States from its position of dominance in areas such as chip-making equipment and biotechnology.

Although Beijing sought to downplay "Made In China 2025" when the plan became a source of friction in the current trade war, it has not altered the vector on which it intends to develop. For instance, China nearly monopolizes global production of rare earths used in advanced electronics such as smartphones and digital radars, and it produces over three-quarters of the world's lithium-ion batteries—the critical technology powering electric vehicles. Some authorities contend that China's ultimate goal is to become the global leader in advanced technology by the hundredth anniversary of the founding of the People's Republic in 2049.

If successful, China's technology strategy would be severely detrimental to U.S. security. In the words of the Pentagon's most recent annual assessment of Chinese security developments, "China seeks to become a leader in key technologies with military potential, such as AI, autonomous systems, advanced computing, quantum information sciences, biotechnology, and advanced materials and manufacturing." Since 2015, Beijing has pursued an official policy of "civil-military fusion" in which the lines between civilian and military segments of the economy are blurred by the sharing of technology. In other words, transactions between foreign companies and Chinese commercial firms can easily result in advanced technology finding its way to the People's Liberation Army.



None of this is unusual in a country seeking to develop from a backward, largely agrarian economy to an advanced, innovation-driven economy in two generations. Beijing's technology strategy echoes policies embraced by the United States during its own development. What is different about China, other than its vast size, is that it is a communist dictatorship. Much of the nation's industry is owned by the state, and all of it is subject to state direction. The Chinese government seeks to control and restrict use of the internet within its borders. Moreover, China's long-term aspirations

require displacing the United States from its position of economic and military dominance, first in East Asia, and later around the globe.

The United States still has important advantages over China. For instance, its chip-manufacturing technology is so advanced that withholding access may hobble Chinese efforts to lead buildout of 5G communications around the world. Its aerospace industry, both civil and military, is far more advanced than that of China. But this may be the last generation in which such statements can be made, because China is progressing steadily in its efforts to match U.S. technology, even in internet services, and the American response has been uneven at best. If Washington is to prevent the current century from becoming "The Chinese Century," it must sustain a world-class technology sector capable of competing across the full spectrum of advanced industries.

China and Russia employ cyberattacks and other illegal means to steal U.S. intellectual property.

China's aspiration to achieve technological dominance is understandable. Many of the market-distorting measures Beijing undertakes to build up its domestic technology sector, such as subsidies and tariffs, are employed by other industrial nations even though they are in conflict with trade commitments. What puts China in a class by itself, however, is the extensive, state-supported use of illegal means to secure access to the intellectual property and trade secrets of U.S. technology companies. As of mid-2020, the U.S. Federal Bureau of Investigation (FBI) had over a thousand cases of technology theft by China under investigation.

FBI Director Christopher Wray told a Washington audience in July of 2020 that Beijing's heavy use of espionage and cyber intrusions targeting U.S. companies has resulted in "one of the largest transfers of wealth in human history." Wray said the value of the property stolen "almost defies calculation," but most experts estimate its long-term worth in the hundreds of billions of dollars, with a corresponding loss in U.S. jobs. Some of these jobs are in the defense industry, but China targets intellectual property

across every segment of the U.S. technology sector. Its goal clearly is to compress the amount of time required for China's own tech sector to catch up with and surpass America's.

For example, Chinese agents targeted the business secrets of U.S. aerospace suppliers even as those suppliers were contributing content to its first indigenous commercial jet, with the apparent intent of displacing such companies with domestic sources. Google disclosed in 2010 that it had suffered "a highly sophisticated and targeted attack" on its corporate infrastructure originating in China "that resulted in the theft of intellectual property"—at the same time Google was providing the operating system for most of China's cell phones.

These attacks follow a pattern in Chinese behavior of gaining access to U.S. technology by fair means or foul, and then working to undermine the business interests of the enterprises that developed the technology. The pattern repeats so frequently that it must be a reflection of official policy, supported by government funding. The number of hackers employed by the Chinese government is estimated at 50,000-100,000, making Beijing by far the biggest source of intellectual property theft in the world.

While cyber theft seems to be the most common tool employed by Beijing for illegally appropriating foreign technology, its espionage efforts are diverse and multifaceted, including recruiting trusted insiders at technology companies, surreptitious copying of patented innovations, and the subversion of academic research. In 2020 the chair of Harvard University's chemistry and chemical biology department was charged with attempting to conceal cooperation with a Chinese program aimed at securing technical information. Similar charges were leveled in 2019 against a biological engineering professor at Virginia Tech.

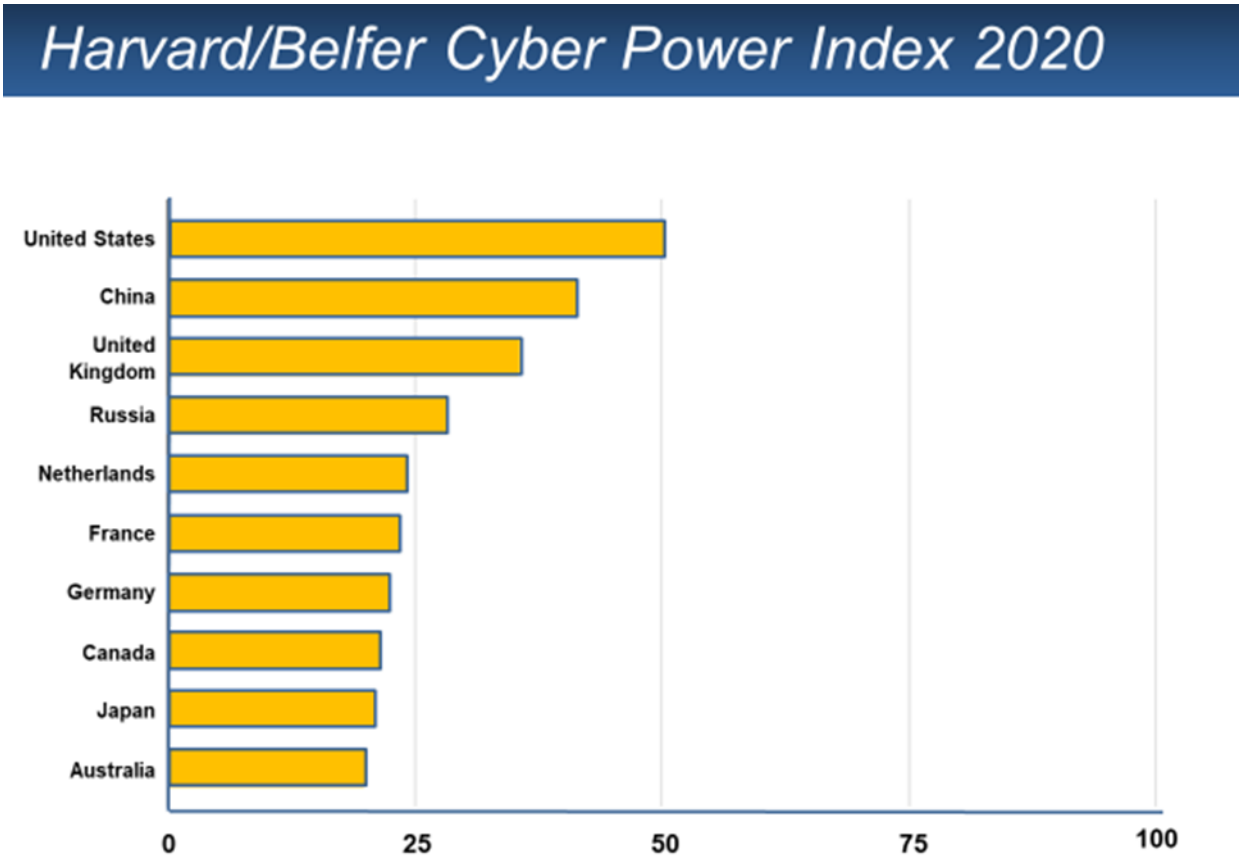
However, China is by no means the only country whose cyber and espionage activities pose a threat to U.S. security. Russian espionage in the United States predates World War Two, and appears to have gotten a major boost from the advent of the internet. In September of 2020 Microsoft disclosed that Russia is the biggest source of state-sponsored attacks on its

customers. That same month, the U.S. government revealed that hackers apparently working in support of Russian military intelligence used novel malware to penetrate the networks of a federal agency and steal sensitive information. The targeted agency was not identified, but undoubtedly is just the latest in a lengthy roster of public and private organizations against which Russian operatives have perpetrated cyberattacks.

Moscow has multiple reasons for mounting such efforts. First, it wants to appropriate U.S. intellectual property for application to its own military capabilities. Second, it wants insight into U.S. military plans and vulnerabilities. Third, it seeks to learn information about Americans in sensitive positions who might be targets for other types of espionage activity. Fourth, it seeks to disrupt operations of the U.S. political system including its electoral processes, and sow distrust within U.S. society. As in the case of Beijing, Moscow does not rely solely on information technologies to perpetrate its attacks, but there is little doubt that the information revolution has given Russian operatives increased options for penetrating and disrupting the U.S. government and technology sector.

One challenge in sorting out the scope and nature of Russian cyberattacks is that state-sponsored hacking often seems to overlap with the work of criminal elements operating within Russian borders. These criminal elements may be used by the Russian government to support its espionage and destabilization campaign. Similar uncertainty surrounds the efforts of other cyber aggressors such as Iran and North Korea. Microsoft estimates that Iran is the second biggest source of state-sponsored attacks against its systems, and North Korea's hacks of sites within the U.S. have been widely reported. So while China may be the biggest source of efforts to steal U.S. intellectual property, it is not alone in seeking to erode the foundations of America's economic and military success.

The biggest challenge in preventing such aggression resides not in the skill of foreign hackers but in the openness of American society. Fortunately, America's robust technology sector provides solutions that do not compromise freedom or prosperity.



Cybersecurity is an indispensable feature of the nation's technology sector.

China is the biggest perpetrator of cyber attacks against the U.S. military and technology sector, but it is far from being the only one. Many states and non-state actors attempt to exploit the growing interconnectedness of information systems and technologies to steal U.S. secrets, impair national security, degrade economic performance, or achieve criminal gain. Because the current era of technological progress is defined almost entirely by the spread of information technologies, possessing the means to protect such resources is essential to an effective security posture.

This is one reason why issues surrounding cyber insurance and cyber risk management have become a central concern for both the public and private sectors. The Foundation for the Defense of Democracies Center on Cyber and Technology Innovation recently hosted a tabletop exercise with former

government officials, insurance executives and defense industrial base managers that examined case studies of actual cyber events impacting the industrial base. The exercise found that application of cyber business interruption coverage across the Defense Department's supply chain would materially enhance supply chain resiliency.

The cyber challenge unfolds in many ways. For the nation's military, the greatest concern is that cyber attacks might be used to damage U.S. warfighting capabilities and economic performance during conflicts. For instance, cyber attacks could be used to collapse the domestic power grid, shut down communications, disrupt financial markets, degrade medical services and otherwise damage the sinews of a nation that is dependent on its networks and information devices to function. Such attacks might also be directed at undermining the performance of warfighting systems that rely on microelectronics and digital connectivity for their effectiveness. A typical Army brigade contains 2,000 devices utilizing signals from the Global Positioning System, which explains why the Pentagon is investing heavily in bolstering the cybersecurity of GPS satellites and ground stations.

In peacetime, cyber intrusions can be and are used to steal data that enables foreign militaries to counter U.S. warfighting systems. This data can be exploited both to improve enemy systems and to identify operational weaknesses in U.S. systems. Once malware is implanted in the hardware, software or network connections of vital systems, it may not be detected for long periods of time, during which it compromises the security of those systems or lies dormant awaiting the moment when it can be activated to have maximum destructive effects on U.S. capabilities.

The military and most large corporations grasped the importance of cybersecurity long ago, following a series of spectacular intrusions perpetrated mainly by foreign players. However, because new applications for information technology are constantly proliferating and the options for compromising those technologies are so numerous, it is hard to keep up with the evolution of the threat. Thus, many of the advances that the military hopes to make using technologies like artificial intelligence,

autonomous vehicles and big data are potentially at risk. The new technologies can not only be degraded, they can be subverted to pose a threat to their users.

The implication of such dangers is that a robust cybersecurity industry is required to protect and enable all the other advances promised by the information revolution. No sector of a digital, connected economy is safe without proper cyber protections. During the recent pandemic, Chinese agents sought to steal intellectual property associated with the search for a vaccine, and criminal elements attacked the on-line learning systems of schools. The anonymity of the internet empowers every type of perpetrator, because it is relatively easy to conceal where an attack originated, or to fabricate an electronic trail, leading investigators to the wrong source. Some speculative scenarios envision wars being provoked by the clever use of cyber tools to encourage the mis-attribution of aggressive acts.

With so many actors around the world pursuing cyber exploits against the U.S., it is hard to anticipate all the future challenges that might arise, much less counter them. Planners can't imagine all the ways in which the "internet of things" or the wireless networks controlling robotic systems might be subverted. The only apparent solution to this danger is to foster a world-class cybersecurity industry that is closely partnered with other segments of the technology sector.

Conclusion: The United States will lose its status as the world's leading economic and military power if its technology sector falters.

This report began by noting that technology shapes every facet of national security. It determines whether the nation possesses sufficient economic resources to compete with other nations; it impacts the quality of military equipment and training; it shapes the ability of popular culture to influence the values of other nations; it even drives socio-economic trends that are the foundation of who Americans are as a people. In short, technology and

the economic sector that produces it are the most dynamic force driving the future of our civilization.

Many, perhaps most, Americans understand this. However, for many years the preeminence of American technology in the world has been taken as a given. That preeminence can no longer be assumed. China is working to dethrone America from its status as the sole global superpower, and so far every step it has taken to achieve that end has been successful. If Washington does not rethink its policies, this may be the last generation that can legitimately claim that America leads the world in economic and military power. Protecting the culture of innovation centered in the nation's technology sector is central to preserving the American future.

An honest assessment of what needs to be done must begin by recognizing that many of the challenges America faces are home grown. We cannot blame other nations for the fact that our tax system often penalizes entrepreneurship, that our scholastic test scores trail most of the developed world, or that our immigration policies impede the ability of industry to attract talent from other countries. If countries such as China are catching up with America, that is due in part to the fact that America has not done enough to stay ahead. For all its achievements, the U.S. technology sector needs help from Washington to stay ahead, especially in five areas.

Federal monitoring. The government's ability to track technology trends is antiquated and balkanized. Much critical data is not collected, and even when it is the current system makes it hard to find or analyze. For instance, it became apparent during the recent pandemic that no federal agency could definitively state how dependent the U.S. is on China for vital pharmaceuticals. When such basic information is lacking, it is impossible to determine what policy responses are required. Washington needs to consolidate and integrate its mechanisms for understanding what is happening in the U.S. technology sector, and how that compares with what is happening elsewhere.

Tax policy. Policymakers are understandably leery about the possibility of intervening in the marketplace to pick winners and losers. When it comes

to new technology, there is no guarantee that government will choose wisely—even in the military realm, which is its exclusive preserve. But in the absence of a massive federal presence comparable to what other countries undertake in their own economies, additional steps must be taken to nurture a culture of innovation. Tax policy, meaning in particular the treatment of research and investment spending, traditionally has been the most fruitful way of fostering private-sector innovation. Washington needs to scrutinize corporate taxation to encourage a maximum degree of technology investment and innovation.

Regulatory burdens. American political culture tends to reward losers and penalize winners. Mismanaged industries long past their zenith often receive hefty federal benefits while new industries that have made good are the object of suspicion. The recent spate of antitrust investigations into the nation's biggest technology companies is a case in point. These companies are critical to the nation's future competitiveness. Amazon isn't just an online sales enterprise, it is one of the world's foremost innovators in areas like cloud computing. Google isn't just a big search engine, it conducts cutting-edge research in everything from neural networks to autonomous vehicles. Exposing such companies to unnecessary regulatory burdens and novel interpretations of antitrust law weakens the forces of innovation shaping America's future.

Property protection. China's rise has been accompanied by massive theft of American intellectual property. U.S. military commanders in the Pacific say that the Chinese often weaponize and field that property faster than the U.S. does, even though the insights originated in America. While the technology sector has made big strides in implementing better cybersecurity, there is more Washington can do to help. Until recently, little was done to penalize companies like Huawei that may have benefited from the misappropriation of U.S. intellectual property. Sanctions against foreign actors who aim to undermine the competitiveness of U.S. technology companies need to be a bigger and more consistent feature of federal policy. Washington's response to the threat of espionage and cyber

intrusion shouldn't be aimed just at the perpetrators—it should also be aimed at the foreign companies that benefit from illegal behavior.

Trade policy. America contains only four percent of the world's population. If the U.S. technology sector is to thrive, it must export. Maybe the items it exports will be goods, maybe they will be services, maybe they will be intellectual property. But without foreign markets, the tech sector cannot remain competitive. Unfortunately, there has been resistance in Washington to funding the kind of export credit system that every other major nation possesses, and as a result U.S. companies often do not compete on a level playing field with their foreign counterparts. Other countries provide much more export assistance than the U.S. government does, and unlike in America the assistance often does not need to be repaid. The U.S. technology sector needs to receive the same treatment that tech companies elsewhere enjoy.

There are many nuances to technology trends and policies, but the one big conclusion is not in dispute. If America does not have a world-class technology sector, then its national security will be gravely diminished. Military preparedness, economic performance, and cultural influence will all suffer. In the current era, new technology denominates success, and no country that falls behind can hope to remain a first-class power.

Funding for the preparation of this white paper was provided by the American Edge Project. The American Edge Project is a coalition dedicated to the proposition that American innovators are an essential part of U.S. economic health, national security and individual freedoms.