2020 Economic Security Assessment

U.S. Department of Homeland Security; Office of Strategy, Policy, and Plans; Trade and Economic Security

Homeland Security

U.S. Department of Homeland Security
Office of Strategy, Policy, and Plans
Office of Trade and Economic Security

Contents

With honor and integrity, we will safeguard the American people, our Homeland, and our values.

Foreword

U.S. commerce, including the movement of goods and transactions, are a vital part of everyday life in America. The daily exchanges of goods and currency that drive the U.S. economy are underpinned by expectations of secure and resilient domestic production, the ability to freely trade, and enough disposable income to support an acceptable standard of living now and in the foreseeable future. These expectations both contribute to, and are dependent on, a secure economic future. It is a necessary precondition for investments in public health and safety, the maintenance and modernization of infrastructure, and financial market stability. Economic security is national security.

During a crisis—like that presented by COVID-19—threats to economic security are clarified, and the inability to secure access to food, medicine, or even the ability to conduct business creates scars on society, and damages both the current state and future potential of the economy. For at least the past decade, U.S. adversaries, particularly China, exploited supply chains for enrichment of their businesses and furtherance of geopolitical goals. It is an action that has harmed not only the United States but also our allies and partners. While the United States remains the global economic leader, hostile economic practices from our adversaries threaten U.S. national security and competitiveness, possibly pushing U.S. companies out of entire markets. Considering these risks, DHS Office of Strategy, Policy, and Plans (PLCY) created the Trade and Economic Security (TES) sub-office to examine economic trends through the lens of national security. TES will propose policies to counter these threats and ensure policymakers proactively manage this risk moving forward.

I am pleased to present the following: "2020 Economic Security Assessment" to the public. The development of this assessment was a DHS-wide effort led by TES. This is the first annual assessment; it will outline the current state of the global economy, the strategic efforts of the United States, and the results therein on greater economic security. Additionally, it will examine current and future trends these efforts produced.

DHS maintains many lines of work, building upon the successes of efforts across the rest of the U.S. Government, to identify and mitigate vulnerabilities in the U.S. supply chain, including medical supply chains. The goal of these efforts is to reduce reliance on adversarial countries for goods and services. DHS has the unique ability to identify such risks in real time and be proactive in responding to them. By using its enforcement and acquisition capabilities, DHS can identify and help incentivize the relocation of supply chains and provide support to our interagency partners who have the capabilities to assist in moving these supply chains into the United States and other trusted countries. DHS monitors for, shares information about, and coordinates responses to cyber threats and threats to critical infrastructure domestically. We are bringing the full suite of our capabilities to bear to ensure supply chains are diverse, secure, and resilient to ensure our nation has a prosperous economic future for many years to come.

Scott L. Glabe;
Senior Official Performing the Duties of Under Secretary; Assistant Secretary for Trade and Economic Security; Office of Strategy, Policy, and Plans

"We directly support economic security every day here in the Homeland by keeping commercial airline travel safe and secure, facilitating commercial trade through our ports of entry, keeping our networks free from economic disruptions and safeguarding our ports and inland waterways that process nearly 90% of all goods coming into our country."

- Acting Secretary Chad Wolf, State of the Homeland, September 9, 2020

Executive Summary

In 2020, DHS established the Trade and Economic Security (TES) sub-office within the Office of Strategy, Policy, and Plans (PLCY) to synchronize the Department's significant operational capabilities and streamline its policy coordination process. This report represents a collective understanding of U.S. economic security by DHS and is intended to drive policy actions across the government to strengthen U.S. global economic standing and secure supply chains.

The COVID-19 pandemic accelerated many technological trends of the 21st Century, bringing forward greater reliance on transformative new technologies. This trend further validated many digital economy giants, solidifying these titans in the global marketplace. Yet, the pandemic also laid bare some growing gaps in the U.S. economy, particularly around manufacturing and supply chains for tangible goods. While the economy is currently on a path to recovery, uncertainty about future trends persists.

TES identified the following key trends that shaped the global economic landscape in 2020, further detailed in the assessment:

1. The United States continues to be the global economic leader. Techonolgoical innovation within the critical domains is crucial to continue to drive this leadership.
2. The People's Republic of China is rising using a combination of hostile economic practices and an industrial policy that, if left unchecked, will threaten the future of U.S. economic security. These practices give China a disproportionate advantage in global influence over competitors who seek to uphold both the text and spirit of the rules-based international economic order.
3. The COVID-19 pandemic caused a severe economic shock that significantly hindered economic growth in 2020 as global commerce was disrupted and borders closed. This pandemic was also a real-time "stress test" of global supply chain dependences particularly for medical supply chains.
4. The integration of high-tech systems into traditional infrastructure shows transformational economic promise, but also introduces cyber vulnerabilities to those same systems increasing risks of stolen intellectual property, illicitly acquired data, and disruption of national critical functions. These risks endanger the future of U.S. economic prosperity if proper steps are not taken to secure the systems.

5. Supply chain dependences on single, sometimes adversarial nations create access chokepoints and vectors for inflicting non-economic actions with a geopolitical agenda, posing significant risk to the integrity of systems and the long-term availability of goods if access is disrupted.

TES views economic security through the lens of several "critical domains" which are derived in part from the National Critical Functions. This report goes a step further to highlight trends, risks, and U.S. Government efforts to mitigate risk to each of the following domains for which TES identified as critical to U.S. economic security:

- ***Critical Manufacturing, Industrial Security and Resilience***
- ***Telecommunications, Cybersecurity, and Data Protection***
- ***Intellectual Property Rights***
- ***Transportation of People and Goods***
- ***Research and Development of Emerging Technologies***
- ***Position, Navigation, and Timing (PNT) Infrastructure***
- ***Power and Electricity Distribution and Storage***
- ***Healthcare and Medicine***
- ***Food and Agriculture***

Though the United States is poised to continue its global economic leadership, competitor nations, particularly China, are increasingly using strategic and predatory trade and business practices to bolster their own industries and leverage them for further geopolitical gains. These actions threaten to supplant U.S. global leadership and are designed to reduce overall U.S. competitiveness in global markets. To ensure that the United States has a secure, resilient, and prosperous economy today, tomorrow, and into the future, it is imperative to proactively mitigate risks in these domains to minimize the opportunity for adversaries to exploit them. As a start, TES highlights in this report significant current risks that policy actions can help remedy to avoid significant economic disruption.

Trade and Economic Security Sub-Office Overview

The DHS Trade and Economic Security (TES) sub-office is organizationally situated within the Office of Strategy, Policy and Plans (PLCY). TES establishes policies that enable the lawful flow of goods and services, people and capital, and information and technology across our borders; and position DHS to effectively counter threats to U.S. entities engaged in global commerce. TES is comprised of four teams: Economic Security Policy, Analysis and Assessments, Trade Policy, and Foreign Investment Risk Management.

ECONOMIC SECURITY POLICY:

The Economic Security Policy team formulates strategies, informed assessments, and policies intended to safeguard the economic security of the United States across a wide range of markets and sectors. The team leads the establishment of DHS policy in this area by unifying its existing authorities and developing a strategic purpose and direction for future state, persistent engagement with both U.S. Government and industry stakeholders. Additionally, the team develops products and policies in close collaboration with the interagency and private sector to scope industrial policy risks and vulnerabilities.

ANALYSIS AND ASSESSMENTS:

The Analysis and Assessments team coordinates with DHS Components and Offices to proactively determine and address strategic threats to the U.S. economy. The team supports TES collaboration with the interagency to better posture its resources and formulate government-wide strategy and direct policy activities throughout the Department.

TRADE POLICY:

The Trade Policy team is responsible for developing strategy, policy, and procedures to facilitate lawful trade while enforcing U.S. trade laws. This team collaborates closely with partners in U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and the interagency on cross-cutting trade issues that include but are not limited to intellectual property rights, forced labor, cargo security,

exports, and digital trade. The team leads the development of regulations, statutes, and policies that reach across DHS Components and require a unified DHS approach. This team also manages the Department's international trade approach, including the negotiation of free trade agreements and the coordination of messaging to foreign counterparts.

FOREIGN INVESTMENT RISK MANAGEMENT:

The Foreign Investment Risk Management Team coordinates DHS risk analysis for, and participation in, two operational national security committees that identify, assess, and mitigate national security risks arising from foreign investment. The Committee on Foreign Investment in the United States (CFIUS) addresses risks to national security arising from foreign direct investment in U.S. businesses, while the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom) advises the Federal Communication Commission (FCC) on the national security and law enforcement concerns arising from granting foreign persons certain telecommunications licenses.

Economic Security Trends in 2020

In 2020, the United States remained the largest economy in the world mostly due to a legal regime and economic practices that facilitate innovation. Though it is poised to continue this leadership, competitor nations increasingly use predatory trade and business practices to bolster their own industries. These actions threaten to supplant U.S. leadership and influence in many key sectors driving down U.S. market competitiveness. In addition, the COVID-19 pandemic disrupted a thriving global economy and brought the world into a period of uncertainty. It exposed pre-existing vulnerabilities in global supply chains and exacerbated hostile economic practices by U.S. adversaries. TES identified several key trends that defined the global economy in 2020.

1. The United States continues to be the global economic leader. Techonolgoical innovation within the critical domains is crucial to continue to drive this leadership.

The U.S. continues to dominate the global economy in 2020 as it has for several decades prior. The 21st Century ushered in the digital era, bringing transformative new technologies that underpin modern society and creating some of the most successful businesses in the global marketplace. The U.S. legal regime and market-based economic practices contribute to continued innovative successes. Innovations in traditionally non-connected domains and the introduction of emerging technologies mostly led by the United States, like artificial intellegence, additive manufacturing, the spread of the Internet of Things (IoT) facilllitated by 5G technology, and advances in biotechnology--position the United States to continue innovation leadership into the future.

2. The People's Republic of China is rising using a combination of hostile economic practices and an industrial policy that, if left unchecked, will threaten the future of U.S. economic security. These practices give China a disproportionate advantage in global influence over competitors who seek to uphold both the text and spirit of the rules-based international economic order.

The current state of the global geopolitical order can be characterized by great power competition. While the U.S. economy is strong, adversarial countries are increasingly taking steps to undermine U.S. economic leadership. China is one such adversary that attempts to leverage its own growing economic strength to undermine the security of the United States and that of its allies and partners. China uses a suite of tactics including theft of intellectual property, strategic foreign investments for geopolitical rationales investments, and industrial policy that violates the spririt, if not the letter of international commercial law, to bolster the competitiveness of its own companies as they seek to penetrate markets. These practices exemplify an ongoing economic competition between liberal democratic, free-market, rule-of-law nations such as the United States and its allies and partners, and authoritarian, state-led capitalist nations like China.

3. The COVID-19 pandemic caused a severe economic shock that significantly hindered economic growth in 2020 as global commerce was disrupted and borders closed. This pandemic was also a real-time "stress test" of global supply chain dependences particularly for medical supply chains.

The COVID-19 pandemic disrupted strong economic progress, shuttering businesses and putting millions of people out of jobs. The free flow of goods and services slowed as borders closed indefinitely to stop the spread of the virus. The U.S. unemployment rate

quickly rose early in the pandemic. It exposed key supply chain dependences on foreign countries. China was the world leader in production of personal protective equipment (PPE) and the epicenter of the pandemic, making the rest of the world's access to PPE challenging as China was able to plan ahead with asymmetrical knowledge of what would be needed. Moreover, the U.S. economy, being heavily dependent on domestic consumption and benefitting from a much larger contribution to gross domestic product (GDP) from the services sector, was affected to a much greater extent than countries centered on manufacturing and growth through exports of goods.

The U.S. economy stabilized in the second half of 2020, with the unemployment rate steadily decreasing each month. Current models predict a return to more normal economic levels by late 2021, depending in part on widespread distribution and administration of one or more COVID-19 vaccines. During this crisis, businesses accelerated the movement of operations online, leveraging telecommunications and cloud-based technologies to allow for continuity. It is worth noting that not only did COVID-19 have an abbreviated direct effect on China's domestic economy for 2020, the levels of exports to the United States from China actually increased, due in part to the shift in U.S. consumption away from services and toward larger numbers of tangible goods.

4. The integration of high-tech systems into traditional infrastructure shows transformational economic promise, but also introduces cyber vulnerabilities to those same systems increasing risks of stolen intellectual property, illicitly acquired data, and disruption of national critical functions. These risks endanger the future of U.S. economic prosperity if proper steps are not taken to secure the systems.

Technology continues to be a driving force for global economic growth. The rollout of 5G infrastructure in many western democracies, including the United States, brings with it a new era of connectivity, powering emerging technologies like the Internet of Things and artificial intelligence. In 2020, technology became even more ingrained in society as the COVID-19 pandemic moved daily business and government operations online, highlighting the importance of telecommunications and cloud-based services for seamless continuity. State-sponsored cyber threat actors from China, Russia, Iran, and North Korea, and cybercrime actors at large, seized upon this new environment to increase cyber-enabled economic and financial exploitation. Examples of this behavior include theft of COVID-19-related treatment and vaccine research; development

material from pharmaceutical companies and global health organizations; and ransomware attacks against hospitals and other COVID-19 treatment facilities. Most notably, in December 2020, it was found that U.S. Government federal networks and private company networks were breached by threat actors who exploited vulnerabilities in the SolarWinds Orion IT management software, potentially giving the perpetrators illicit access to private communications and sensitive activities. As the adoption of 5G infrastructure and other key technologies accelerates in the approaching post-COVID-19 world, ensuring the security and resilience of connected systems from compromise will remain of utmost importance.

5. Supply chain dependences on single, sometimes adversarial nations create access chokepoints and vectors for inflicting non-economic actions with a geopolitical agenda, posing significant risk to the integrity of systems and the long-term availability of goods if access is disrupted.

The COVID-19 pandemic showed that the United States is, in many cases, overly dependent on a single nation or small region for key materials in critical supply chains. Several supply chains, from critical minerals, to semiconductors, to PPE, are reliant upon suppliers and manufacturers in China. For example, roughly 90 percent of all supply and processing of Rare Earth Elements (REEs), an essential component in key consumer and defense technologies, comes from China.[1] China also controls significant segments of global supply chains through active state intervention in markets, ultimately driving global prices below profitability for U.S. and other western economies. This tilting of the playing field leads to a disproportionate share of manufacturing taking place in China and/or under China's control, and a slow decline of U.S. capabilities. These dependencies create chokepoints where, in the event of a disruptive event, like the COVID-19 pandemic or a military conflict, China can cut off supply to the rest of the world, causing severe harm to U.S. industries, consumers and allies. Moreover, the vulnerability presented by such concentrated supply transcends the narrower threat of intentional harm, as countries may still restrict exports in the face of spiking demand due to self-interest or rational business decisions. As policy makers apply lessons learned from the COVID-19 crisis, it is important to look beyond just the virus and PPE and seek to diversify a broad range of supply chains where there are concentrated dependencies. Such actions will foster competition and minimize risks of access disruption.

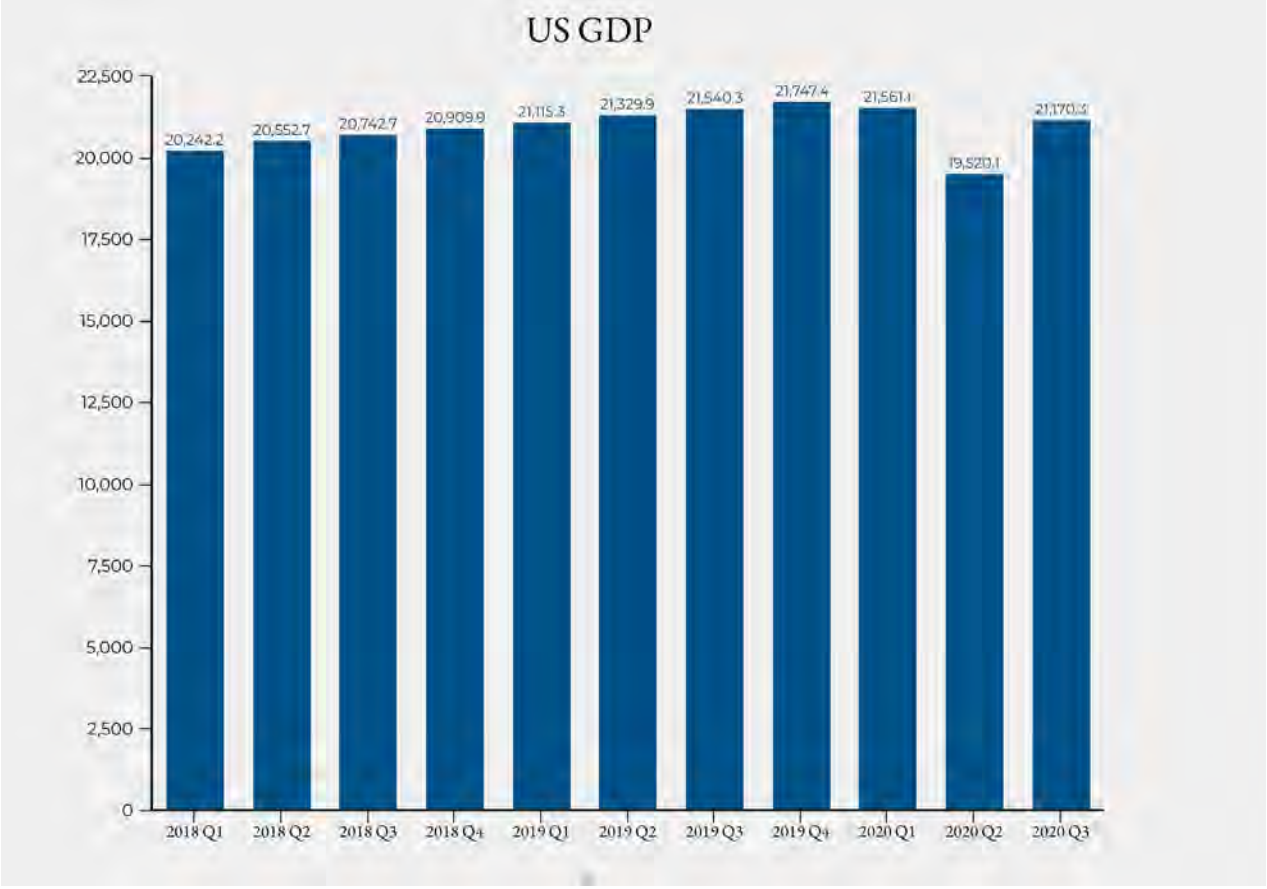
U.S. Position in the Global Economy

The United States continues to drive the world's largest economy, even as it pushes through the effects of the COVID-19 pandemic[2], but, the disruptions in global commerce caused by COVID-19 resulted in one of the most severe contractions in the U.S. economy in recorded history.[3] Quarters 1 through 3 demonstrate a GDP slump that coincided with global lockdown orders; however, GDP is currently trending back upwards. Trade in goods and services also suffered because the United States both imported and exported significantly less than in 2019 overall. Many other nations suffered to a similar extent as a result of the pandemic, though trends of competitor nations' foreign direct investment in parts of key export supply chains and competitiveness with U.S. firms continue. Government investment in the U.S. economy briefly spiked due to the implementation of the CARES Act.[4] The U.S. economy is on a path of continued improvement, but the pandemic revealed fresh concerns over global economic relationships.

FIGURE 1 – U.S. GDP BY QUARTER FROM 2018 to 2020

[Billions of dollars] Seasonally adjusted at annual rates

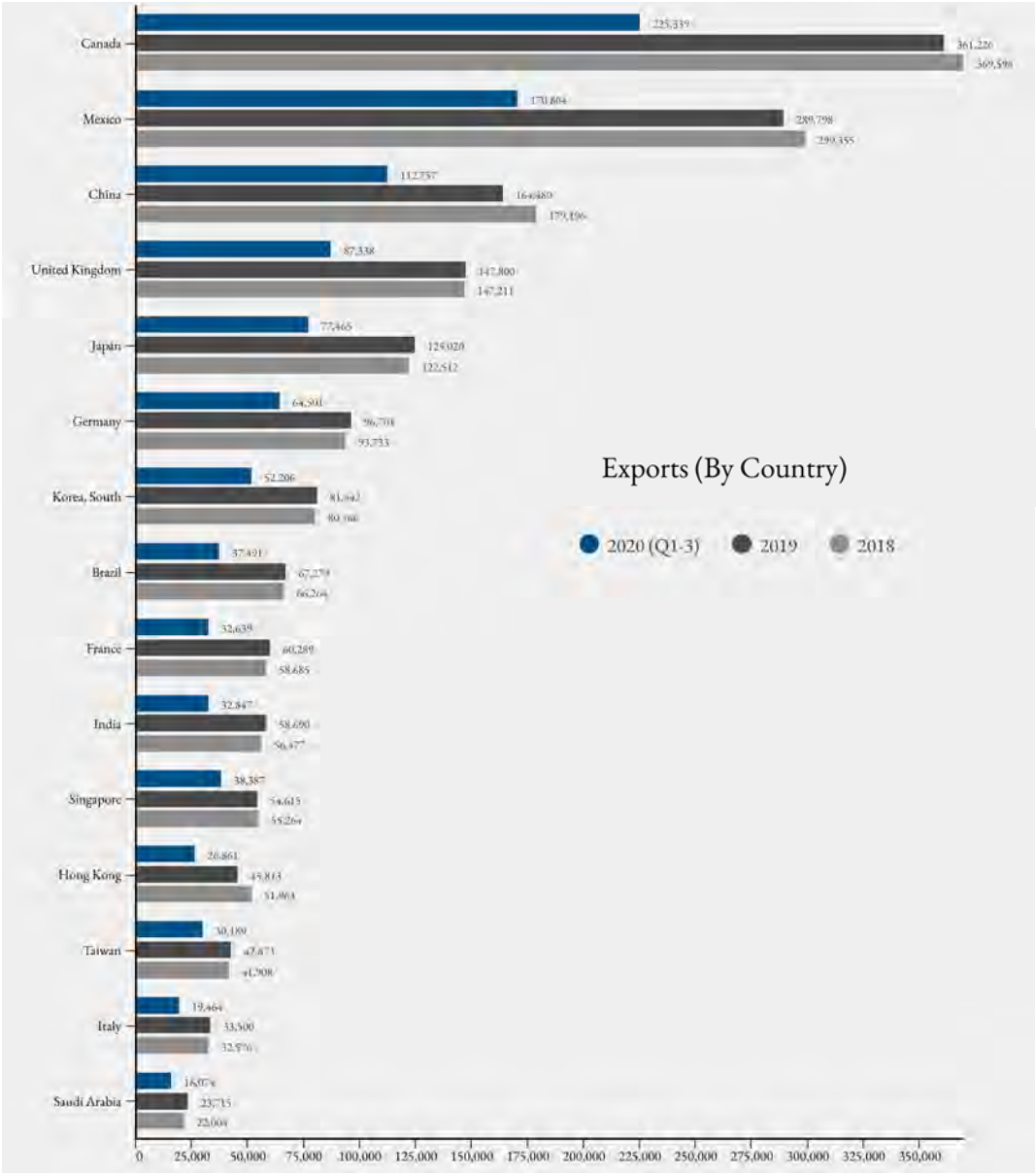
Source (US Bureau of Economic Analysis)



U.S. Exports:

The COVID-19 Pandemic caused U.S. export totals to decline from 2019 levels. This is due in part to the first order effect of closing ports around the world, reducing the movement of people, and shuttering international services in order to lessen the spread of the virus. As the world begins to open back up to international trade and travel, the expectation is that we will see a rise in U.S. exports to previous levels. There may even be a near-term increase in exports as a percent of overall trade, coming partially from stimulus-related currency fluctuations that make the dollar cheaper abroad, and thus put a slight tailwind behind U.S. exports. This is an aspect that we will continue to monitor throughout 2021.

FIGURE 2 – U.S. EXPORTS AND NATIONS TO WHICH U.S. EXPORTS
Source (US Census Exhibit 20- U.S. Trade in Goods and Services by Selected Countries and Areas - BOP Basis)

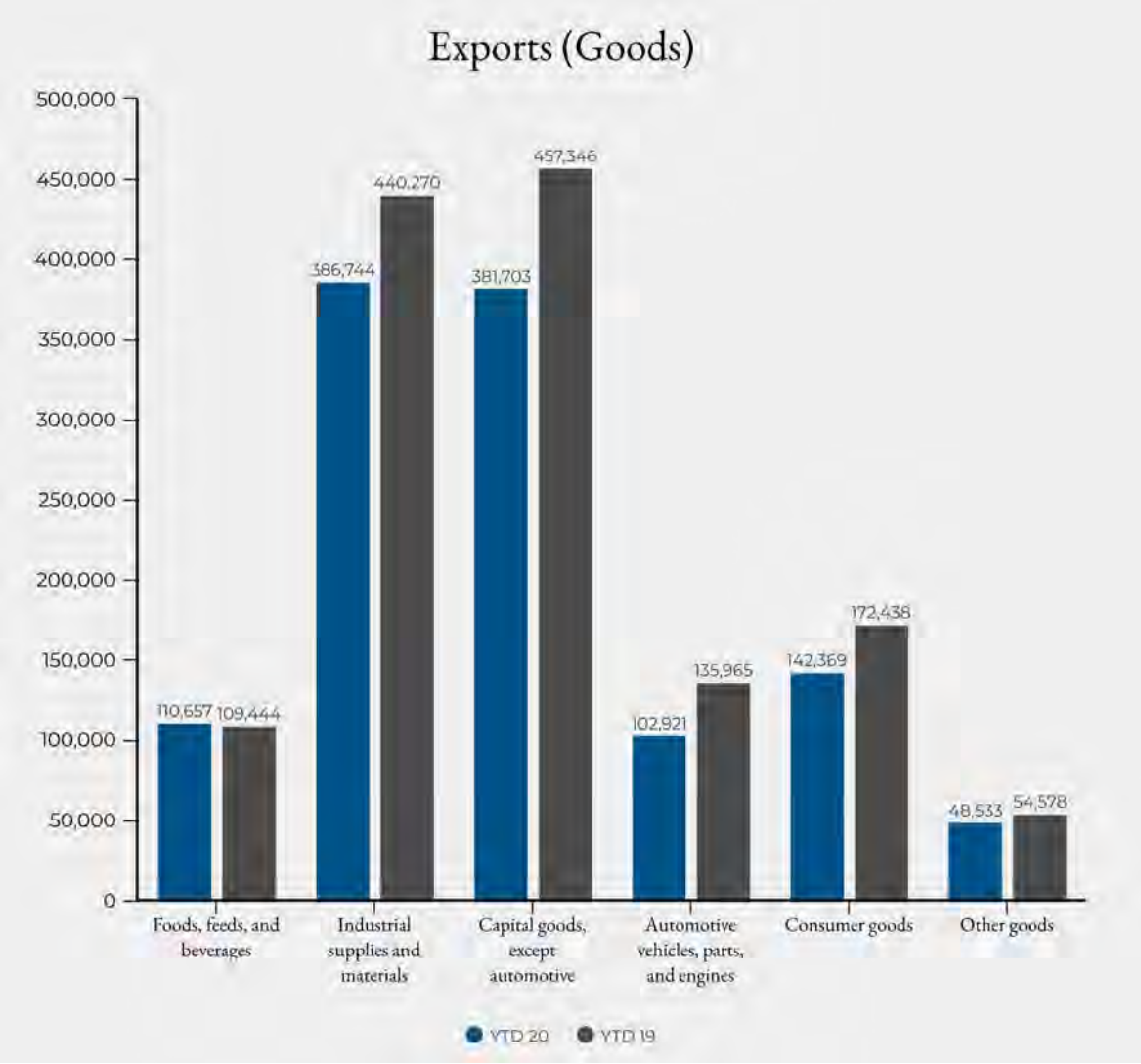


Export of Goods:[5]

Exports of industrial materials were the highest yielding category in 2020. Industrial materials include crude and refined oil, plastic materials, natural gas, nonmonetary gold, precious metals, and more. U.S. exports of industrial materials for Quarters 1 through 3 in 2020 totaled $345.8 billion. Exports of capital goods without counting automotive goods were the second highest yielding category in 2020. If automotive goods are counted, capital goods become the top U.S. export category. In this category are industrial machines, telecommunications equipment, semiconductors, computers, aircraft, medical equipment, commercial vessels, and more. This category accounts for $342.6 billion in exports. Automotive vehicles, parts, and engines exports to date account for $90.2 billion.

FIGURE 3 – U.S. EXPORTS OF GOODS BY END-USE CATEGORY AND COMMODITY

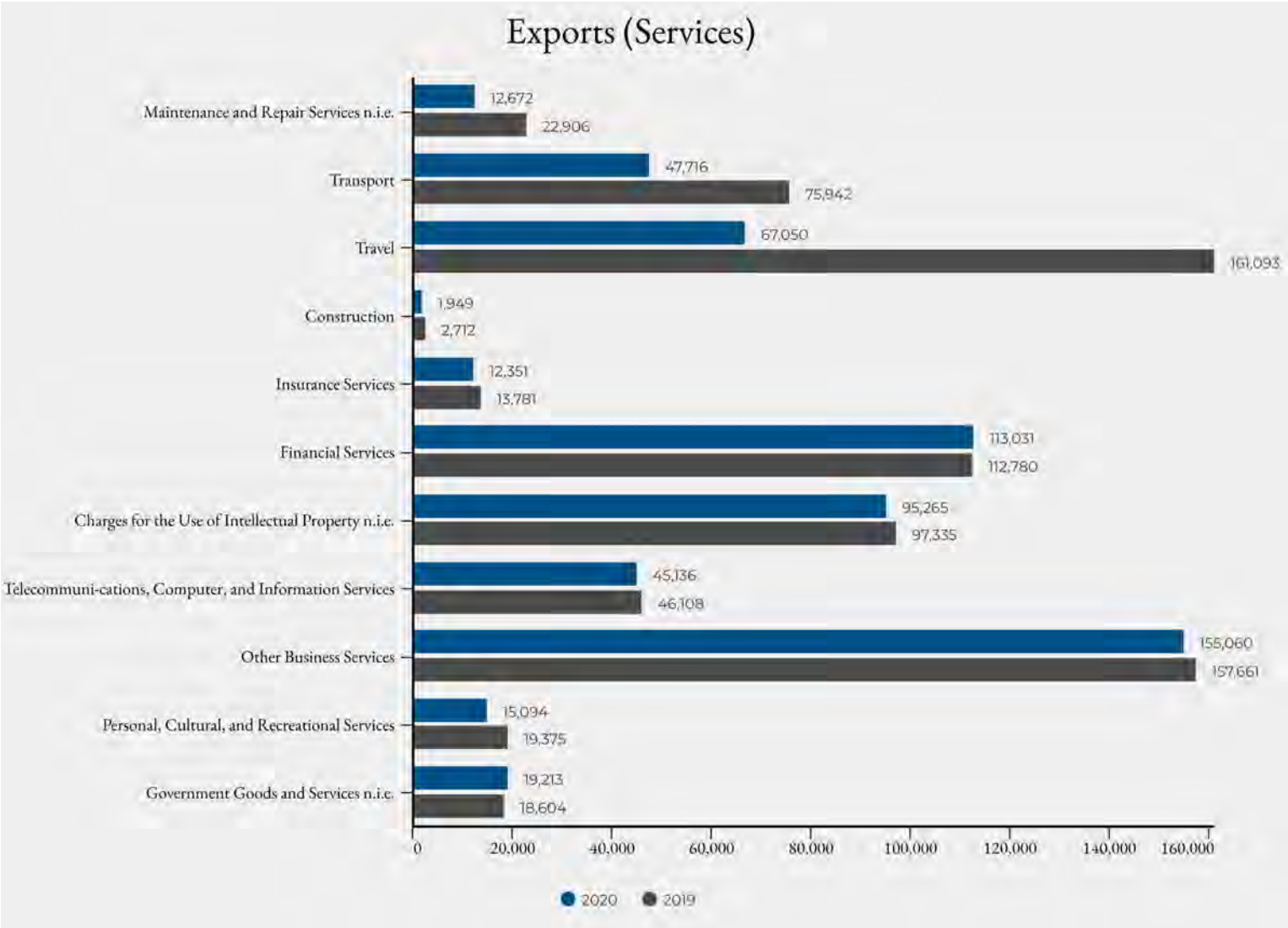
Source (US Census Exhibit 7- U.S. Exports of Goods by End-Use Category and Commodity)



Export of Services:[6]

Finally, exports of services for the first three quarters in 2020 amount to $516.9 billion. In the services category, financial services were the top U.S. export category for the first three quarters in 2020, amounting to $98.9 billion. At this time in 2019, financial services exports totaled $101.4 billion, showing a slight decline in financial services exports in 2020. The second highest category of services exports for the first three quarters of 2020 are charges for the use of intellectual property, which amounted to $80.4 billion. At this time in 2019, these exports amounted to $87.4 billion, demonstrating a more significant decline. Only government goods and services experienced an increase from $16.6 billion in 2019 to $17.2 billion in 2020, which can be attributed to the COVID-19 pandemic response.

FIGURE 4 – U.S. U.S. EXPORTS OF SERVICES
Source (US Census Exhibit 3- U.S. Exports of Services)



Competitor Nations:

Other top economic powers in the world include China, Japan, Germany, India, France, and the United Kingdom. Except for China, the other countries represent a bloc of U.S. allies or partners, many of whom are party to trade agreements with the United States. China, on the other hand, is one of the staunchest competitor nations that threatens the overall global competitiveness of the United States, leveraging strategic investments related to its Belt and Road Initiative and Made in China 2025 strategy. While the United States is a key exporter of industrial materials and capital goods, particularly those related to finished telecommunications and computer equipment, China exerts significant control of elements within their supply chains. For example, while the United States exports a significant number of semiconductors, China is the global leader of semiconductor manufacturing. Further, China is a principal miner and processor of rare earth elements and other critical minerals benefitting from looser environmental restrictions that preclude the United States and other competitor nations from participating in the same process. Though manufacturing of U.S. goods is slowly shifting out of China into other Asian countries, in some part due to U.S. trade policy, China's market share for manufacturing is still significant enough to warrant concern over dependence.[7] China controlled a significant percentage of PPE supply chains related to the COVID-19 pandemic, hindering distribution around the world and exposing a need for supply chain diversification. A similar need is indicated in other sectors in which China controls significant portions of the supply chain.

Competition Issues Stemming from the People's Republic of China:

China is a large U.S. strategic competitor militarily, technologically, and especially economically. China's effort to modernize both its economy and military resulted in several specific actions aimed at propping up its own companies and industries. Two examples of these efforts include the Belt and Road Initiative (BRI) and Made in China 2025 (MIC2025). The BRI is aimed at capturing large markets focusing on infrastructure and trade, particularly from Asia to Europe, and achieving maritime superiority to protect shipping routes. Made in China 2025 is aimed at improving innovation and manufacturing. Practically, these initiatives provide direct government financial support and investment into key markets and industries, enabling Chinese-owned firms to undercut fair market prices, putting them at an advantage in the global market.

1. https://pubs.er.usgs.gov/publication/pp1802O
2. Trend analysis taken from: Table 1.1.5. Gross Domestic Product, National Income and Product Accounts, National Data, Bureau of Economic Analysis, U.S. Department of Commerce, https://apps.bea.gov/iTable/iTable.cfm?reqid=19&step=2#reqid=19&step=2&isuri=1&1921=survey.
3. According to data supplied by the Bureau of Economic Analysis at the U.S. Department of Commerce, the decline in U.S. GDP so far in
4. Final Report of the Economic Security Subcommittee, Homeland Security Advisory Committee, November,16, 2020, https://www.dhs.gov/publication/economic-security-subcommittee.

Huawei and NucTech are two examples of Chinese companies that benefit from Chinese government investment.[8] Other firms, particularly U.S. firms, have a smaller footprint in the market and have difficulty competing. Both firms also exemplify hostile practices of leveraging market penetration to proliferate vulnerability-ridden products that could potentially be exploited by the CCP to capture data for use in its extensive surveillance apparatus. In the case of Huawei, United States efforts have successfully swayed allies to shift away from Huawei as a telecommunications provider, including the United Kingdom and Japan; and other countries like Brazil are actively considering such a move.

China's strategy of military-civil fusion, where it seeks to create and propagate dual-use technologies for the benefit of both its commercial and defense sectors, makes it difficult to distinguish the affiliations of its firms. This system allows China to exploit U.S. capital and technologies to enable the development and modernization of its military industrial complex, financed in part, through civilian resources. To combat this, on November 12, 2020, President Trump issued Executive Order 13959 Addressing the Threat from Securities Investments That Finance Communist Chinese Military Companies issuing sanctions and prohibiting U.S. persons from investing in those companies.

Data Practices of the People's Republic of China

China has a storied history of leveraging cyber-enabled means of intrusion for intellectual property and technology theft, resulting in the loss of billions of dollars to U.S. businesses. Now, it seeks to codify potentially malicious data practices to give its companies greater competitive advantages when harnessing that data. Currently in effect, its Cybersecurity Law requires companies operating in China to store their data within the geographical borders of China;[9] and its National Intelligence Law requires companies to submit relevant information and data to the Chinese security apparatus without allowing those companies to inform their customers.[10]

By the end of 2020, two other laws are set to take effect – its Data Security Law and its Cryptography Law – both of which will provide the Chinese government with easier access to data, including foreign-held data.[11] These laws in tandem provide a powerful legal mechanism through which the government can gain access to sensitive data, making it easier for China to integrate relevant data into their own systems for economic benefit or for its extensive surveillance infrastructure.

Emerging Regulatory Regimes:

Amidst these trends, new regulatory regimes comprised of both existing and newly issued authorities emerged in the United States to mitigate risks to United States national and economic security, particularly responding to threats posed by foreign adversaries.

- *Committee on Foreign Investment in the United States.* The Committee on Foreign Investment in the United States (CFIUS) is a forum in which the U.S. Government identifies and mitigates risks to national security arising from foreign investment. The authorities of CFIUS were greatly increased by Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) by expanding the jurisdiction of CFIUS to address the growing national security concerns of foreign exploitation of certain investment structures that traditionally fall outside of CFIUS jurisdiction. Additionally, FIRRMA modernizes CFIUS's processes to better enable timely and effective reviews of covered transactions and identifies critical technologies as a focus point for investment review.
- *Federal Acquisition Security Council.* The Federal Acquisition Security Council (FASC) is led by the Office of Management and Budget (OMB) and brings together senior leaders from across the government to better protect U.S. government acquisition of ICTs.
- *Information and Communications Technologies Supply Chain Risk Management Task Force.* The Information and Communications Technologies Supply Chain Risk Management Task Force is the nation's first public-private partnership for managing risks to the Information and Communications Technology (ICT) Supply Chain.
- *EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom).* Signed on April 4, 2020, this EO formalized the Team Telecom working group that advises the Federal Communications Commission on risks to national security and law enforcement interests and the security, integrity, and availability of U.S. telecommunications networks.
- *EO 13873 ICT Supply Chain Securing the Information and Communications Technology and Services Supply Chain*. EO 13873 was signed on May 15, 2019, to

5. All statistics derived from: Exhibit 7 - U.S. Exports of Goods by End-Use Category and Commodity, U.S. International Trade in Goods and Services, U.S. Census Bureau, https://www.census.gov/foreign-trade/Press-Release/current_press_release/index.html.
6. All statistics derived from: Exhibit 3-U.S. Exports of Services, U.S. International Trade in Goods and Services, U.S. Census Bureau, https://www.census.gov/foreign-trade/Press-Release/current_press_release/index.html.
7. https://www.kearney.com/operations-performance-transformation/us-reshoring-index/full-report.
8. Huawei is a PRC-owned telecommunications infrastructure firm that is the global leader in providing mobile telecommunications equipment, particularly for 5G technology. NucTech is a screening and surveillance company used to scan personnel for security and cargo for shipping.

reduce reliance on untrusted ICT suppliers with a history of exploitative practices.

- *EO 13920 Securing the United States Bulk-Power System*. Signed on May 1, 2020, this EO declares threats to the bulk-power system by foreign adversaries constitute a national emergency. Serving as the backbone of our nation's energy infrastructure, the Bulk-Power System (BPS) is fundamental to national security, emergency services, critical infrastructure, and the economy.

U.S. Critical Domains

The Trade and Economic Security (TES) sub-office views U.S. economic security through the lens of domains that are critical to ongoing operation and growth of the U.S. economy. Each of these domains represents a category that is essential for the economy to function, so much so that disruption of one of them will have severe negative economic consequences. They also represent sectors that will benefit greatly from emerging technologies that will shape the future of global society.

TES developed this list by identifying the industries, emerging technologies, and infrastructure that are needed for a robust and growing economy, as well as any supply-constrained resources upon which those industries and technologies rely. TES distilled this research and analysis to produce an initial list of U.S. critical domains with descriptions outlining their importance to the U.S. To assist in this identification step and refine the list, TES incorporated feedback from the DHS Trade and Economic Security Policy Council (TESPC), consulted with select external stakeholders within the U.S. Government, and performed internal, focused analysis to fill any remaining information gaps.

Within each domain, TES will assess identified key risks both under the current state, desirable conditions, and under "stress tests" of potential future state scenarios. Guided by subject matter experts in both DHS and the wider interagency, TES looks at supply chains, production, processing, and manufacturing methods, foreign government influence, asset ownership, and tangential relationships to identify vulnerabilities associated with each identified critical domain risk.

Finally, TES will, over time, track and designate each domain on a spectrum of priority. This spectrum ranking will be flexible, noting that although each critical domain was selected because it is a high priority to DHS for their long-term economic security implications, though certain domains may be trending up or down at different times.

9. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/
10. https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf
11. Data Security Law information: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-data-security-law-draft/. Cryptography Law information: https://thediplomat.com/2019/10/decoding-chinas-cryptography-law/.
12. 2021 Manufacturing Industry Outlook, Deloitte US, https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/manufacturing-industry-outlook.html.
13. For Quarter Two statistics, see: https://www.bls.gov/opub/ted/2020/manufacturing-labor-productivity-decreased-15-point-5-percent-in-the-second-quarter-of-2020.htm. For overall information, see: https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/manufacturing-industry-outlook.html.
14. https://www.aei.org/multimedia/defense-production-act-production-tracker/.

CRITICAL MANUFACTURING, INDUSTRIAL SECURITY, AND RESILIENCE

The critical manufacturing sector includes primary metals, machinery, electrical equipment appliances and components, and transportation equipment. On its own, this domain is a significant contributor to GDP, and its importance is amplified by the fact that many of the outputs are imbedded in other aspects of our nation's critical infrastructure, including electrical distribution, mining, ports and transportation. The United States must ensure both its own robust manufacturing capability or its ability to rely on a trusted network of allies and partners for continued production and supply of intermediate goods and services. In addition, access to the materials and technological inputs necessary to manufacture key industrial products must keep pace with the rapidly advancing technology landscape to sufficiently meet demand.

Critical manufacturing also includes mining and processing of minerals that are necessary to produce certain high-tech finished products. These minerals, like cobalt, lithium, graphite, copper, and rare earth elements, not only need to be mined but also processed and refined from ore into useable material. The manufacturing process, particularly for smaller devices, requires the use of specialized, precision manufacturing capabilities.

Risks:

Declines in domestic mining, refining, production, and manufacturing in the United States pose significant economic risk to this critical domain. Higher labor and regulatory costs in the United States encourage businesses to outsource manufacturing to low cost nations with fewer legal protections for people and businesses. Some countries like China have built robust mining and mineral processing sectors through a lack of environmental restrictions coupled with geographic access to critical mineral deposits. As a result, China is a prime economic competitor in this space, dominating the market for processing critical minerals from ore to refined product, and then again from refined product to intermediate and finished goods. The rest of the world is reliant on China to process and manufacture usable materials. This reliance creates a chokepoint for material access that can be exploited, whether to meet domestic demand or simply to disadvantage competitor nations. This level of control also allows for price manipulation of the raw and intermediate goods, which can then be used to further

create reliance on China as a manufacturer and supplier. Finally, state-led investments in domestic manufacturing in China aligned with its Made in China 2025 Strategy creates longer-term demand signals, which further solidify China's manufacturing dominance.

2020 Developments:

Due to the COVID-19 pandemic, the manufacturing industry declined in 2020. Border closings and global lockdown orders negatively impacted manufacturing output. U.S. industrial production fell 16.5% and factory orders fell 22.7% in 2020 compared with 2019.[12] Like in other sectors in 2020, employment in the manufacturing sector fell overall in 2020 with a sharp decline in Quarter 2 and a recovery in Quarter 3.[13] While manufacturing employment is on the road to recovery, it is still lower than pre-lockdown levels in February. Related to COVID-19, the implementation of the Defense Production Act (DPA) in 2020 resulted in U.S. manufacturing firms increasing

Example: Electric Vehicle Battery Manufacturing

Electronic vehicle (EV) batteries are an instrumental innovation for automobile technologies, enabling a shift toward greater energy efficiency, and reduced reliance on oil and other hydrocarbon-based fuel. Yet, like many transformational technologies that are paving the road to future, EV batteries have complex supply chains, including numerous inputs and processes from harvesting natural resources and processing them into highly-refined materials, to manufacturing and assembly of finished goods and then finding markets. Mastering EV battery manufacturing is key to secure future markets for U.S. economic prosperity.

While EV batteries show tremendous transformative potential—with implications beyond just the EV market—there are several immediate concerns about their development and production that might hamper U.S. economic and national security. Not only does the United States have critical dependences for intermediate goods in this supply chain, but also China dominates production of battery-grade raw materials, accounting for 80% of total global output in 2019. [17] This dominance can be, at least partially explained by lower environmental standards for a highly polluting refinement and manufacturing process. China leads in other segments of the EV battery supply chain producing 66% of anodes and cathodes (the two critical pieces for EV battery functionality) and controls 73% of global output of lithium-ion battery cell manufacturing in 2019.[18] These critical dependences along the EV battery supply chain present immediate issues of access and production efficiency. Taken in the context of a growth industry, they lead to the potential for reduced supply, shipping disruptions, and lack of certainty—especially in times of crisis or conflict. In addition, human rights violations and environmental concerns cloud the extraction and refining of certain raw materials like cobalt that are necessary for batteries to function. Advances in large battery technology and the manufacturing of those technologies will not only benefit the U.S. passenger vehicle industry along with over-the-road trucking and last mile delivery, they will form the cornerstone for enabling affordable micro-grids, smart buildings and a multitude of alternative power solutions.

production of PPE and non-medical equipment needed for pandemic response.[14] The rollout of multiple COVID-19 vaccines in late 2020 means manufacturing of vaccines will probably rise to meet the scale of global demand.

The U.S. Government continued efforts from the White House's 2018 "Strategy for American Leadership in Advance Manufacturing" which not only aims to bolster the U.S. manufacturing sector towards greater global competitiveness, but also prioritizes the development of manufacturing technologies themselves, which the United States succeeds in exporting. The U.S. Government is also continuing efforts from Executive Order 13817 A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals (December 20, 2017) and the subsequent Executive Order 13953 Addressing the Threat to the Domestic Supply Chain from Reliance on Critical Minerals from Foreign Adversaries (September 30, 2020). EO 13817 aims at strengthening every stage of the critical minerals supply chain including mining and extraction, refining, and manufacturing and integration into intermediate goods.[15] EO 13953 furthers those efforts by specifically focusing on lessening U.S. reliance on foreign adversaries, particularly on China, for supply of critical minerals.[16]

INFORMATION AND COMMUNICATIONS TECHNOLOGIES AND DATA PROTECTION

Information and Communications Networks are the backbone that powers the 21st Century digital economy. Domestic and international infrastructure, like land cables, undersea cables, and constellation satellites enable data to flow across borders and provide access to communications networks. Both public and private infrastructure and networks must be securely and efficiently managed and data that flows through those networks must be securely stored. Key technologies in this domain include mobile network infrastructure, routing, emerging technologies, and data storage and processing services.

Risks:

U.S. communications networks have proven to be vulnerable to cyber-enabled intrusions, unauthorized monitoring and intercept, physical sabotage, compromised technology within their systems, and mismanagement. ICT service disruptions have negative economic consequence as they temporarily halt the provision and use of

15. https://www.federalregister.gov/documents/2017/12/26/2017-27899/a-federal-strategy-to-ensure-secure-and-reliable-supplies-of-critical-minerals
16. https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-domestic-supply-chain-reliance-critical-minerals-foreign-adversaries/
17. https://www.benchmarkminerals.com/membership/china-controls-sway-of-electric-vehicle-power-through-battery-chemicals-cathode-and-anode-production/
18. https://www.benchmarkminerals.com/membership/china-controls-sway-of-electric-vehicle-power-through-battery-chemicals-cathode-and-anode-production/
19. https://www.cyberstates.org/
20. https://www.state.gov/european-court-of-justice-invalidates-eu-u-s-privacy-shield/

critical services. Untrusted hardware providers present particular risk due to proven vulnerabilities and low-quality engineering which could be used for backdoor access to governments or criminals. Data is similarly vulnerable to cyber threat actors, mismanagement, economic and business practices that enable illicit data access and exploitation.

U.S. data and computing services abroad are particularly vulnerable to governments that compel access to the data. Unlike for ICT networks, except in the most severe consequences, exploitation or misuse of data will not result in physical damage to systems. However, it often aligns with efforts to misappropriate technology, or inflict economic and reputational damages. Exploiting these vulnerabilities can provide network traffic information that is valuable for foreign intelligence gathering and enable the theft of intellectual property and trade secrets. Mitigating risks to ICT, software, and data storage is challenging because development often outpaces a company's or an individual's ability to secure them.

Hardware providers from China now dominate the international market for mobile network infrastructure. Their success is punctuated by effectively using predatory business practices--like using subsidies to undercut market prices--, that make U.S. alternatives less competitive. These same companies are subject to China's legal regime that enables it to compel access to data traversing networks, and also use equipment that is poorly engineered and riddled with known vulnerabilities. Their prolific use internationally makes shifting away from them challenging for nations with a desire for next generation mobile networking. Compounding risks from China's data collection legal regime are competition risks from a combination of industrial policies as the Belt and Road Initiative, Made in China 2025, and the Digital Silk Road projects, all of which target ICT systems as sector for growth.

Finally, as businesses and society increasingly move online due to COVID-19 lockdowns, the integrity of ICT and data storage systems become ever more important. Disruptions by cyber threat actors become potentially lucrative as facilities like hospitals and response facilities are targeted by ransomware and other cyber-enabled means for extorting payment. With a massive increase in multinational business being conducted in the virtual space, the opportunities for corporate espionage are growing too.

2020 Developments:

In 2020, the U.S. IT sector is projected to reach $1.9 trillion in revenue adding 330,000 jobs.[19] The COVID-19 pandemic lockdowns resulted in a shift of personal, commercial, and government activities to online settings leveraging virtual meeting and cloud environments. This trend resulted in additional bandwidth strains on network infrastructure due to increased traffic. The pandemic did not impact this sector as much as other critical domains, but it still resulted in global revenues falling roughly $1 trillion short of early year projections.

Other developments in 2020 include the invalidation of the EU-U.S. Privacy Shield by the European Court of Justice, creating potential impediments on the free flow of transatlantic data the principal means for trade in services.[20] The U.S. Government is prioritizing a remedy for this issue as alternative means for cross-border data flows are cumbersome and expensive, and hinder small to medium sized businesses. Also, late in December 2020, the SolarWinds Orion IT management software breach was discovered, and cyber threat actors used it to enter U.S. Government systems and private sector networks. Threat actors were able to successfully access troves of sensitive government; however, the full scale of the breach is still unknown. Although the scale and scope of the breach is still unknown, data highlights a need for improved federal cybersecurity efforts.

The U.S. Government is continuing efforts from Executive Order 13873 Securing Information and Communications Supply Chains. New strategies were issued such as the White House's "National Strategy to Secure 5G" and the Cyberspace Solarium Commission's Final Report recommendations. Both strategies targeted the ICT sector and placed emphasis on securing and diversifying ICT supply chains. Amidst U.S. pressure on the international community to shift away from untrusted 5G providers, more U.S. allies in 2020 announced plans to shift away from these providers.[21] On December 22, TES released a data security business advisory warning companies of doing business with Chinese data service and infrastructure providers due to its business practices and legal regime that enables China's government to access company data.[22]

21. https://www.solarium.gov/public-communications/supply-chain-white-paper
22. https://www.dhs.gov/news/2020/12/22/dhs-warns-american-businesses-about-data-services-and-equipment-firms-linked-chinese.
23. U.S. Government Accountability Office, Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market (Jan. 2018), https://www.gao.gov/assets/690/689713.pdf.
24. U.S. Government Accountability Office, Intellectual Property: Agencies Can Improve Efforts to Address Risks Posed by Changing Counterfeits Market (Jan. 2018), https://www.gao.gov/assets/690/689713.pdf.

INTELLECTUAL PROPERTY RIGHTS PROTECTION

The protection of intellectual property rights (IPRs) is at the bedrock of the U.S. innovation-based economy. Strong intellectual property protection of patents, copyrights, and trade secrets promotes innovation and encourages businesses toward long-term idea generation as well as short-term profit maximization. Protecting IPRs is critical to provide incentives to companies to engage in costly research and development, ultimately leading to the creation of new, market-expanding products. Enforcement of IPRs in an international market, while more difficult than domestic enforcement, is a necessary cog in the incentive structure, and key to protecting the ongoing competitiveness of U.S. firms that engage in international business. The U.S. Government works within itself, with like-minded countries, and through international organizations to propagate and enforce a strong IP regime for global commerce.

Risks:

The unlicensed manufacture and sales of products that are otherwise covered by IPRs can be a highly lucrative endeavor as it avoids the sunk costs of research and development. Failure to protect and enforce IPRs abroad provides a competitive edge to companies that operate in the lax enforcement jurisdiction. Online third-party marketplaces, if lacking adequate enforcement and vetting of sellers, are a catalyst for IPR violations as they facilitate the international sale of IPR infringing goods without accepting responsibility for the role played by the marketplace in the transaction. The effect has been particularly harmful to innovative small and medium-sized U.S. businesses. In addition, as trademarks serve as a proxy for communicating quality to consumers, counterfeit goods, in many cases, introduce poor quality and dangerous items to the U.S. economy, leaving consumers susceptible to the health and safety dangers associated with such.[23]

Although slightly different in nature, the forced sharing of trade secrets in exchange for market access, industrial espionage, and network intrusions are other mechanisms through which a foreign entity can skip the investment in R&D and go right to commercialization stage. For example, China often leverages stolen intellectual property or forced technology transfer for its commercial and military industries.[24]

25. Exhibit 3. https://www.census.gov/foreign-trade/Press-Release/current_press_release/index.html
26. https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods
27. https://www.whitehouse.gov/briefings-statements/administration-issues-joint-strategic-plan-intellectual-property/
28. https://www.reuters.com/article/us-ema-cyber/hackers-steal-pfizer-biontech-covid-19-vaccine-data-in-europe-companies-say-idUSKBN28J2Q7
29. https://www.ttnews.com/articles/ports-shipping-industry-responsible-26-us-gdp-study-says.
30. https://unctad.org/news/covid-19-cuts-global-maritime-trade-transforms-industry
31. https://www.aei.org/china-global-investment-tracker/
32. https://www.federalregister.gov/public-inspection/2020-28031/addition-revision-and-removal-of-entities-from-the-entity-list

2020 Developments:

To date in 2020, entities in the United States received roughly $95.3 billion in charges for the use of intellectual property in a foreign jurisdiction.[25] Early in 2020, TES produced a report on Trafficking in Counterfeit and Pirated Goods which recommends actions that mitigate illicit trade, such as comprehensive "Terms of Service" agreements, efficient notice and takedown procedures, and clearly identifiably country of origin disclosures.[26]

In November 2020, the White House Intellectual Property Enforcement Coordinator issued the United States Joint Strategic Plan on Intellectual Property (2020-2023).[27] The plan brings together enforcement efforts across the U.S. Government, including DHS, to guide engagement with U.S. trading partners, and the private sector to ensure effective use of all legal authorities, expand law enforcement action and cooperation, and engage and partner with the private sector and stakeholders.

During the COVID-19 pandemic, trafficking of counterfeit and IP-violative medical equipment was a problem. CBP successfully seized several of these goods which include N95 masks and testing equipment, to prevent them from entering the marketplace. Cyber threat actors also targeted pharmaceutical and research facilities seeking to exfiltrate intellectual property for the creation of COVID-19 vaccines and treatments.[28]

INTERNATIONAL TRANSPORTATION OF PEOPLE AND GOODS

The transportation of people and goods, via sea, air, and rail, is the principal facilitator for international commerce, and presents a myriad of economic security concerns. When operating effectively, this domain bolsters international business interactions, facilitates innovation, fosters counter-cyclical growth mechanisms, and allows market forces to allocate global resources to maximize productive capacity.

The U.S. economy benefits greatly from the ability to competitively sell goods globally which requires efficient and secure operation of shipping, loading, and customs infrastructure. The government and private sector are also dispensed with the responsibility to screen and protect U.S. buyers from harmful foreign imports. Transparent foreign and logistics data and other operational information is critical to detect and interdict harmful products. Further, tourism and international business travel contributes significantly to the U.S. economy, promoting international retail sales, trade in services, and growth for U.S. business operations. Travel for business or personal reasons requires effective screening of identities and visa applications and monitoring for the transport of illicit goods via people or disruption by terrorists or criminal groups.

Risks:

It is estimated that the ports and shipping industries account for roughly one quarter of U.S. GDP.[29] The main risk to this domain stems from the need to process goods and persons in both an efficient and secure manner. Ports of entry and shipping have significant vulnerabilities in their infrastructure integrity and in screening capabilities due to the sheer volume of cargo and people that traverses through them. Cargo can be harmed by pests, invasive species, chemicals, IP-violative goods, and harmful consumer products. It can be physically tampered with by terrorists or criminal groups. Attacks or disruption of port and shipping infrastructure from criminal or terrorist organization can cause significant damages personal harm. To mitigate these risks, effective cargo and traveler screening at scale is critical without which disruptive goods, criminal actors, and otherwise sick or harmful travelers can traverse ports and borders unhindered. In this setting, dependences on one non-allied source for screening equipment becomes problematic and can provide a foreign government with sensitive cargo information and travel patterns of high-level officials.

33. https://thediplomat.com/2020/11/us-targets-chinas-quest-for-military-civil-fusion/
34. https://www.justice.gov/opa/pr/chinese-national-who-conspired-hack-us-defense-contractors-systems-sentenced-46-months
35. http://uis.unesco.org/apps/visualisations/research-and-development-spending/
36. https://www.hhs.gov/coronavirus/explaining-operation-warp-speed/index.html
37. https://www.scmp.com/tech/innovation/article/3111510/china-tops-world-ai-patent-filings-surpassing-us-first-time

Adversaries seek to harm U.S. interests economically using strategic investments in transportation infrastructure. Domestically, dependences on China for traditional and connected rail infrastructure puts at risk the integrity of national freight shipping and long-term access to rail supply if cut off. China-supplied connected rail infrastructure can provide China's government with cargo IP and personal information. Internationally, China's investments in South and Central American transportation infrastructure pose significant risk to U.S. shipping as it traverses those regions. For example, China's $2.52 billion in investments into transportation infrastructure in Panama are mostly focused along the Panama Canal where the United States accounts for 60% of the canal's traffic. Another risk comes in the form of the PRC's ambitions to build a railway spanning South America, highlighting its continued push of becoming a key player within the transportation domain within the Western Hemisphere.

2020 Developments:

International transportation of both people and goods was significantly hindered due to the economic shock of the COVID-19 pandemic. Efforts to halt the spread of the virus caused exports around the world fell. This means that air and maritime transportation of goods also fell. Maritime shipping fell by 4.9% in 2020.[30] In addition, due to lockdowns enacted to stop people from spreading COVID-19 further, transportation of people also fell. Transit businesses around the world saw revenue fall.

At the same time, China's Belt and Road Initiative (BRI) efforts pressed on with key investments focusing on Transportation. Between 2005 and 2020, China's global investments and associated construction projects related to transportation amounted to USD $378.75 billion.[31] The signing of the Regional Comprehensive Economic Partnership (RCEP) in 2020 means that transportation in the Indo-Pacific region is set to increase due to a reduction in regulatory barriers between signatories. BRI investments steadily flowed into Africa and China was heavily involved in structuring the African Continental Free Trade Area. In the Western Hemisphere, China focuses investments in transportation infrastructure projects, particularly in the Panama Canal, aiming to gain greater economic influence over regional shipping.

The USG is currently addressing BRI threats on a company-by-company basis. For example, on December 18, 2020, after TES had identified the threat presented by Chinese-based security screening company NucTech and worked with U.S.

38. https://finance.yahoo.com/news/baidu-leads-china-artificial-intelligence-132800878.html
39. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-regarding-national-strategy-critical-emerging-technologies/
40. https://www.cisa.gov/pnt 41. http://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo
42. https://www.cisa.gov/publication/pnt-backup-report
43. https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/
44. https://www.cisa.gov/energy-sector
45. https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

Government colleagues to raise the issue with our foreign government partners, the U.S. Department of Commerce added NucTech to the Entity List in addition to several other China-based firms. Commerce cited, among other things, that NucTech's lower performing equipment hindered U.S. efforts to counter illicit international trafficking in nuclear and other radioactive materials. Lower performing equipment means less stringent cargo screening, raising the risk of proliferation."[32]

RESEARCH AND DEVELOPMENT OF EMERGING TECHNOLOGIES

Research and development of emerging technologies is a necessary condition for "innovation," and for truly innovative products, it can take many years to develop and perfect the underlying technologies. Testing, modeling, risk assessments, and evaluations are all part of this process. Final goods and services based on recently emerging technologies—which include artificial intelligent computer vision, 3D printing, autonomous vehicles, gene-editing, mRNA-based vaccines, and other biotechnological advances—all show transformative potential and will reshape entire aspects of critical domains. Many emerging technologies, once fully developed, will be extremely versatile in use and integrated into military and defense platforms. This potential leads governments and private companies to spend significantly on research and development to fund these efforts and raises the value of the consequent IPRs. As a result, it is critical to prevent unauthorized access, theft, and inadvertent technology transfer.

Risks:

Due to the time and capital needed to bring a new technology to market, adversaries often look for opportunities to circumvent these costs by exploiting vulnerabilities to the U.S. research and development domain. To achieve these goals, they resort to tactics like leveraging tools like espionage and insider threats, unauthorized system access, and technology transfers.

Theft of U.S. research and development is common practice and a means to substitute for innovation in countries with closed or declining economies. China, Russia, Iran, and North Korea frequently attempt to exploit this sector by using a combination of espionage, and strategic investment and business practices. The misuse of student or work visas to position illicit foreign agents in key research and development institutions is similarly common. Accelerating the potential harm, China's military-civil fusion strategy means it will use its civilian technologies for military and intelligence purposes raising possibilities of illicit data collection and exploitation by the Chinese government. China's

Central Commission for Integrated Military and Civilian Development aims to "facilitate transfers between the defense and civilian sectors to improve the sophistication of China's military technology, particularly in sectors critical to informationized warfare."[33] In addition, research and development data is particularly vulnerable to cyber threats. Cyber threat actors based in China specialize in exfiltrating key research data that can be integrated into both civilian and defense platforms.[34] Finally, China can use its export markets to provide funding and scale for research and development efforts abroad enabling it to use investment and data gathering activities to fuel its own development of emerging technologies.

2020 Developments:

The United States spends approximately $476.5 billion on research and development.[35] These expenditures account for roughly 2.8% of U.S. GDP. The private sector bears most of the burden of these expenditures accounting for $340.7 billion. The U.S. Government does not spend as much on research and data at present than it did in decades prior, but due to the promise of emerging technologies and current demand, this trend could change. For example, the COVID-19 pandemic led to a rush in research and development investment into treatments and vaccines that required significant government financial support. Operation Warp Speed, a public-private partnership between federal agencies and private firms resulted in hundreds of millions of dollars in grants for the research, development, testing, and rollout of COVID-19 vaccines.[36] At the same time, U.S. COVID-19 vaccine research and development entities combatted attempts to steal IP as countries frantically sought to develop their own treatments.

Government investment in research and development of emerging technologies is key if the United States wishes to maintain competitiveness in the future. China continues its efforts to subsidize research and development of emerging technologies per its civil-military fusion strategy. According to the UN patent agency, in 2020, China surpassed the United States in patent application filings for the first time since the global system was established 40 years ago.[37] The leading company responsible for these patent filings was tech giant Baidu.[38] At the same time, in 2020 the White House issued the "National Strategy for Critical and Emerging Technologies."[39] This strategy promoted the increased investment in research and development of emerging technologies specifically in the ICT sector and emphasized protecting research and technology from theft and other illicit means of acquiring research data.

POSITION, NAVIGATION, AND TIMING (PNT) INFRASTRUCTURE

Position, navigation and timing services is an enabling domain that includes the creation, placement, and uninterrupted use of satellites and other internationally placed sensors that are necessary to ensure the ability to navigate international and domestic airspace and waters. The principal technology in the PNT domain is the Global Positioning System (GPS) in the United States. Other satellite navigation systems in the world include GALILEO (European Union), GLONASS (Russia), and BeiDou (China). PNT services can also be used to track users, measure and monitor weather and nature-related events (e.g., hurricanes, volcano eruptions), and collect data on the Earth in general. Several civil, military, and commercial technologies, services, and critical infrastructure are heavily reliant on the integrity of PNT systems. PNT enables other critical economic domains as it powers communications, information technology, transportation, emergency services, energy, and financial services.

Risks:

DHS identified the reliance on GPS as essentially the sole provider of PNT services in the United States and around the world as a significant risk.[40] As with any technology, sole reliance and lack of back-ups for critical systems means disruption could prove catastrophic. GPS jamming, spoofing, cyber-enabled intrusions, physical sabotage, compromised technology within systems, and operation of U.S. data and computing services in data centers of other countries that compel access to the data all bear significant risk to PNT systems. In addition, military anti-satellite technologies will pose a significant threat to PNT services particularly in the event of a conflict.

2020 Developments:

Almost sole reliance on GPS continues to be a significant vulnerability to the PNT domain and other PNT technologies do sufficiently meet the requirements for effective GPS replacements. While GPS is one of the highest-quality PNT services in existence, complementary capabilities include alternate space-based systems and constellations, terrestrial beaconing systems, time-over-fiber, cellular and wireless signals, and local terrestrial systems. Notably, in 2020 the European Space Agency's alternative to GPS, GALILEO, was scheduled for completion.[41] When fully operational, it will be interoperable with GPS.

DHS issued its "Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)"[42] outlining backup and complimentary capabilities that can be used for resilient PNT systems. Also, President Trump signed "Executive Order 13905 on Strengthening National Resilience Through Responsible Use of Position, Navigation, and Timing" which directs companies seeking to enter in federal contracts to use alternate PNT services to GPS.[43]

POWER AND ELECTRICITY GENERATION AND DISTRIBUTION

Power generation and distribution is one of the most essential elements of critical infrastructure providing the nation with everything from heat to life support systems. The integrity, reliability, and efficiency of the North American Grid and supporting infrastructure is a necessary input, not only for manufacturing, but also the provision of services, research, transportation, and consumer activity.

According to CISA, the U.S. electricity segment contains more than 6,413 power plants (this includes 3,273 traditional electric utilities and 1,738 nonutility power producers) with approximately 1,075 gigawatts of installed generation.[44] More than 80 percent of the nation's energy infrastructure is owned by the private sector. Power infrastructure is divided into three segments: electricity, oil, and natural gas. In addition, access to non-renewable sources of energy to fuel power generation like oil, coal, and natural gas is still the principal concern for continued functionality of power systems. Cross-cutting technologies in this domain include electric grid modernization, systems integration, cybersecurity, subsurface science and technologies, materials, fuel, and energy storage. Development in renewable fuels, electricity storage and battery innovations, and integration of artificial intelligence into industrial control and grid management systems will shape the global economy for decades to come.

Risks:

Access to fuel and enabling technologies for power generation and storage remains high risk as significant exports of non-renewable fuels like oil come from politically volatile regions, like the Middle East. This reliance puts sources and shipping of fuel at risk from adversarial militaries, terrorism, and piracy. Network intrusions by a well-resourced state actor, if ever successful could disrupt the bulk power system leading to sustained outages. Supply chain dependence on China for materials used to manufacture renewable sources

46. https://www.peters.senate.gov/newsroom/press-releases/peters-introduces-legislation-to-address-vulnerabilities-in-medical-supply-chain-bring-critical-manufacturing-back-to-us-and-michigan
47. https://www.peters.senate.gov/newsroom/press-releases/peters-introduces-legislation-to-address-vulnerabilities-in-medical-supply-chain-bring-critical-manufacturing-back-to-us-and-michigan
48. https://www.hsgac.senate.gov/media/minority-media/peters-unveils-new-report-on-lowering-prescription-drug-costs-with-michigan-patients-and-health-care-providers
49. https://www.cfr.org/blog/mapping-chinas-health-silk-road

of energy and energy storage equipment, like electric vehicle batteries, pose access and competition issues to U.S. firms in those industries. In addition, adversarial supply for enabling equipment that is integrated into the power grid is another vector for cyber exploitation. Natural weather patterns like hurricanes, tornadoes, and blizzards frequently disrupt the continued operation of power and electricity generation and distribution causing power outages across the nation.

2020 Developments:

In May 2020, vulnerabilities in the U.S. power and electricity storage and distribution led President Trump to issue the Executive Order on Securing the United States Bulk-Power System.[45] In particular, the EO targets acquisitions of electric equipment supply chain vulnerabilities that exist from reliance on adversary supply of equipment. DHS helps this effort by identifying risk information and risk management practices to inform the procurement of energy infrastructure. It also coordinates with the Department of Energy and interagency partners to issue regulations to secure America's bulk-power system.

HEALTHCARE AND MEDICINE

The United States is the largest market in the world for pharmaceutical company sales accounting for USD $475 billion.[46] As the COVID-19 pandemic highlights, the efficiency of the U.S. healthcare system and biohazard disaster management is dependent on a reliable supply of products that meet U.S. regulatory requirements for safety and efficacy. Brand name drug prices continue to increase and between 2005 to 2015, 78 percent of new drug patents were based on drugs already in existence.[47] The U.S. Government must ensure that the healthcare system and biohazard management function are efficient and resilient. This means supplies of necessary products that meet U.S. regulatory requirements for safety and efficacy must be robust and adequately stockpiled, and supply chains are secure and resilient from adversarial countries.

Risks:

The COVID-19 pandemic exposed supply chain vulnerabilities to the healthcare and medicine sector due to an overreliance on China. China dominated the market for PPE, so when COVID-19 spread to other countries and the United States, those nations were forced to dig into emergency stockpiles that were often insufficient to supply the demand. There are supply chain dependences on ingredients for prescription drugs

sold in the United States, with more than 80% of active pharmaceutical ingredients imported from overseas, principally from China and India.[48] Proliferation of prohibited and counterfeit healthcare materials are also a problem.

China is also aiming to strengthen its position as a global leader in the health care market through its Health Silk Road.[49] It has also turned its attention to the Western Hemisphere with vaccine partnerships in Mexico and donations of medical equipment.

Finally, healthcare and medicine are also vulnerable to cyber threats with hospitals being targeted by ransomware during the COVID-19 pandemic. There is an increased vulnerability for cyber theft of and industrial espionage against research and development information related to medicine with the uptick in such activity to relieve the effects COVID-19 has on people, hospitals, and the economy.

2020 Developments:

China's initial mismanagement of COVID-19 significantly contributed to the current global pandemic, which tremendously strained healthcare providers. The protective actions taken around the world to alleviate COVID-19 had significant and widespread consequences on the economy. During the coming months and years, the economic fallout from these protective actions will continue to grind on health system finances: hospitals must forgo performing lucrative elective procedures, putting healthcare providers in certain regions under economic pressure, and job losses overall will leave patients with no or limited coverage. The combination of these factors creates a negative feedback loop, with reduced revenue leading to closure of less profitable facilities, leading to fewer healthcare jobs, and increased uncertainty of those still employed, further reduce demand in those areas.[50] The continued shutdowns and slow rollout of the vaccine will keep clinics closed and non-urgent visits cancelled, resulting in major lost revenues.[51]

While the CARES Act[52] provided $50 billion in funds to help providers recover, demand for services and revenue decreased, and likely will continue to do so until the economy fully recovers.[52] Based on the four-month period from March to June, 2020, the American Hospital Association estimates a financial impact of $202.6 billion in losses for America's hospitals and health systems.[53]

Digital health and telemedicine became more important in the wake of COVID-19, though digital health and venture capital investment was already rising, growing to $7.4

50. https://www.advisory.com/topics/covid-19/2020/05/covid-19-financial-impact
51. https://www.forbes.com/sites/ellevate/2020/06/04/an-industry-look-at-healthcare-in-the-time-of-covid-19/?sh=9ba20099d90e
52. https://home.treasury.gov/policy-issues/cares
53. https://www.aha.org/guidesreports/2020-05-05-hospitals-and-health-systems-face-unprecedented-financial-pressures-due
54. https://www.cbp.gov/newsroom/national-media-release/cbp-continues-seize-large-number-counterfeit-and-unapproved-covid-19

billion in 2019. COVID-19 accelerated innovation and implementation of telehealth technologies for continuity of care.[53]

Prohibited and counterfeit drugs also remain a problem. As of June 1, 2020, CBP seized more than 107,300 FDA-prohibited COVID-19 test kits in 301 incidents; 750,000 counterfeit face masks in 86 incidents; 2,500 EPA-prohibited anti-virus lanyards in 89 incidents; and 11,000 FDA-prohibited chloroquine tablets in 91 incidents.[54]

DHS, through the Federal Emergency Management Agency (FEMA) Defense Production Act authorities, played a leading role in the nation's whole-of-government approach to the COVID-19 pandemic in ensuring proper stock and distribution of life-saving medical services, supplies, and equipment to state, local, tribal, and territorial partners, service members, and federal agencies.[55]

Foreign government actors are taking advantage of the drive for a return to normalcy as a new venue to obtain sensitive medical intellectual property. IBM released a report claiming that malicious cyber actors are targeting the COVID-19 cold chain, which is a pertinent part of delivery and storage of a vaccine at safe temperatures.[56]

FOOD AND AGRICULTURE

U.S. consumers should have access to safe and nutritious foods, and potable water, which requires U.S. producers to produce a steady and reliable nutrient base. In addition, the agriculture sector is a major source of wealth generation for the U.S. economy through exports. Agricultural exports provide a key counterbalance to the U.S. Current Account, which is heavily influenced by imports. A reduction in U.S. export capacity would cause a greater annual deficit, erode U.S. purchasing power, and ultimately cause either a reduction in the value of the dollar, or a greater need to borrow from foreign sources, or both.

Emerging technologies like artificial intelligence and the IoT allow for precision-based farming, enabling greater efficiency. U.S. consumers must be shielded from increasing risks of disease from imported food and beverages. Digitized and traditional irrigation infrastructure and farming equipment needs to be free from exploitation.

Risks:

U.S. food and agriculture production are vulnerable to a range of threats that are

55. https://www.defense.gov/Newsroom/Releases/Release/Article/2435891/dod-announces-749-million-in-defense-production-act-title-iii-covid-19-actions/
56. https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply
57. https://www.npr.org/sections/goatsandsoda/2020/06/14/876002404/locusts-are-a-plague-of-biblical-scope-in-2020-why-and-what-are-they-exactly

amplified through participation in an international economy. Invasive species and pests, introduced through trade and travel, can devastate harvests, increase fire-related risks to U.S. forests, and propagate disease through insect vectors. Pests pose a unique and significant threat to U.S. crop production as they are a natural threat where avoidance is challenging. The effects pests can have on the agricultural industry are currently playing out in east Africa, where locusts are destroying the crops and food sources of millions of people impacting 10 percent of the world's population. This can have rippling effects across the global agriculture food supply and supply chains.[57]

Food and agriculture are vulnerable to climate change forces that alter crop growth patterns. Invasive species can devastate harvests and access to food, particularly in more impoverished regions of the nation and globally. Other risks include the misuse of global resources, where a lack of global rules and enforcement can lead to negative outcomes for many nations. Examples of this include: the reduction in fish stocks that are under pressure from illegal, unreported, and unregulated (IUU) fishing operations; the overuse of fertilizers, leading to water pollution and potential scarcity of key components.

In addition, the tainting of imported foods, whether intentionally or as a product of substandard foreign regulatory practices, with chemicals and diseases that can result in harmful substances being ingested, inhaled, or absorbed by animals and humans is a big risk. Natural disasters also run the risk of devastating food sources and farms.

Adversarial government participation in western hemisphere economies (e.g., BRI in South America) threatens to spread the market distortions to agriculture trade policies, particularly those of Argentina and Brazil, undercutting U.S. export markets by pairing agriculture exports with favorable financing.

Finally, certain enabling technologies for food production and distribution and agriculture in general are also sometimes vulnerable to risks. Declining irrigation and water infrastructure could result in insufficient water supply to crops. In areas often in drought, this risk is magnified. Connected farming equipment is also vulnerable to cyber threat actors potentially having severe consequences if leveraged at scale.

2020 Developments:

China's failure to abide by the commitments it made in the Phase One trade deal,

combined with the effects of the COVID-19 pandemic has severely harmed the U.S. agriculture sector.

The COVID-19 pandemic began in an open-air food market in Wuhan, China. Downstream effects of the virus have resulted in disruption of the food supply due to lockdown restrictions. Freshly unemployed people and families were unable to receive enough food to sustain them. Other foreign developments include plant-eating locusts that devastated crops in Kenya and several surrounding countries, showing the potentially damaging affects if a similar invasive species were introduced in the United States.[58] The United States donated $19.7 million in humanitarian assistance funds to affected African nations.

With the first cases introduced in 2018, the African Swine Flu is having a significant impact on the global pork market. China holds the largest swine herd; however due to the African Swine Flu, China's herds dropped nearly 40 percent since 2019. This is causing an increase in global demand, which, coupled with the expansion of U.S. processing facilities, is presenting opportunities for the U.S. to extend their reach into the global agricultural market. However, U.S. swine production remains vulnerable to the Swine Flu, which has not yet made significant inroads, due in part to the COVID-19 restrictions.

In the United States, numerous people had mysterious seeds shipped to them, originating from China.[59] The PRC Government assisted the U.S. Department of Agriculture in the identification and interdiction of the seeds. It was unknown if they could have been an invasive plant species or harmful to animals, but now, a sampling of the seeds were identified as a mix of herbs, weeds, fruits and vegetables, and ornamental species most likely resulting from a "brushing" scheme to falsely inflate ratings of other products in ecommerce. The threat, however, was realized that small parcel ecommerce is now a vector to spread invasive species and pests that could decimate U.S. agriculture.

DHS issued grants through its Silicon Valley Innovation Project related to the study of food supply chain security in an effort to help mitigate the disruption of lifeline supply chains.[60] Mesur IO, Inc., the recipient of the grant, aims to expand its existing software to provide CBP with greater visibility into food supply chains. The increased awareness of the importance of the security and continued development of the U.S. agricultural industry is evident by the 370 percent increase in farm tech investments since 2013.[61]

DHS Economic Security Efforts

Considering the significant risks posed to critical domains, the U.S. Department of Homeland Security is participating in several efforts that seek to mitigate these risks and secure the future of U.S. economic security. The creation of the Trade and Economic Security (TES) sub-office to specifically examine risks and explore how best DHS can mitigate them was a significant step. Among all the DHS-specific and intergovernmental risk-mitigating and economic security-promoting actions, TES highlights the following as instrumental in economic security risk mitigation in 2020:

COVID-19 Actions:

The Federal Emergency Management Agency (FEMA) is the U.S. Government leader for COVID-19 pandemic response and supports the Department of Health and Human Services (HHS) to assist state, local, tribal, and territorial (SLTT) partners with related preparedness and response activities. One of the first priorities for FEMA and HHS was to increase the surge capacity of SLTT hospitals: FEMA directed the U.S. Army Corps of Engineers to work closely with SLTT officials to construct Alternate Care Facilities in the event traditional healthcare institutions were filled beyond capacity. FEMA distributed tens of millions in commodities through services such as emergency food shipments and obligated billions of dollars since March 13, 2020, from the Disaster Relief Fund, all to support SLTT partners. It also provides support for consequence management consistent with the U.S. Pandemic Crisis Action Plan.

Through the FEMA COVID-19 Supply Chain Task Force, FEMA is executing a strategy to maximize the availability of critical protective and lifesaving resources by focusing on reducing the medical supply chain capacity gap. To do this, it uses a four-pronged approach of preservation, acceleration, expansion, and allocation to increase supply and expand domestic production of critical resources to account for long-term supply considerations. The Supply Chain Task Force works with major commercial distributors to facilitate the rapid distribution of critical resources to locations where they are needed most. A key example of this partnership is Project Air Bridge. The air bridge was created to reduce the time it takes for U.S. medical supply distributors to receive PPE and other critical supplies into the country for their customers. FEMA covers the cost to fly supplies into the U.S. from overseas factories,

58. https://www.usaid.gov/sites/default/files/documents/1866/07.14.20_-_USAID-BHA_East_Africa_Desert_Locust_Crisis_Fact_Sheet_5.pdf
59. https://www.aphis.usda.gov/aphis/newsroom/stakeholder-info/sa_by_date/sa-2020/sa-07/seeds-china
60. https://www.dhs.gov/science-and-technology/news/2020/10/09/news-release-dhs-awards-193k-enhance-visibility-food-supply-chains
61. https://agfunder.com/research/2020-farm-tech-investment-report/
62. https://www.fema.gov/news-release/20200726/fema-covid-19-el-grupo-de-trabajo-y-la-estabilizacion-de-la-cadena-de

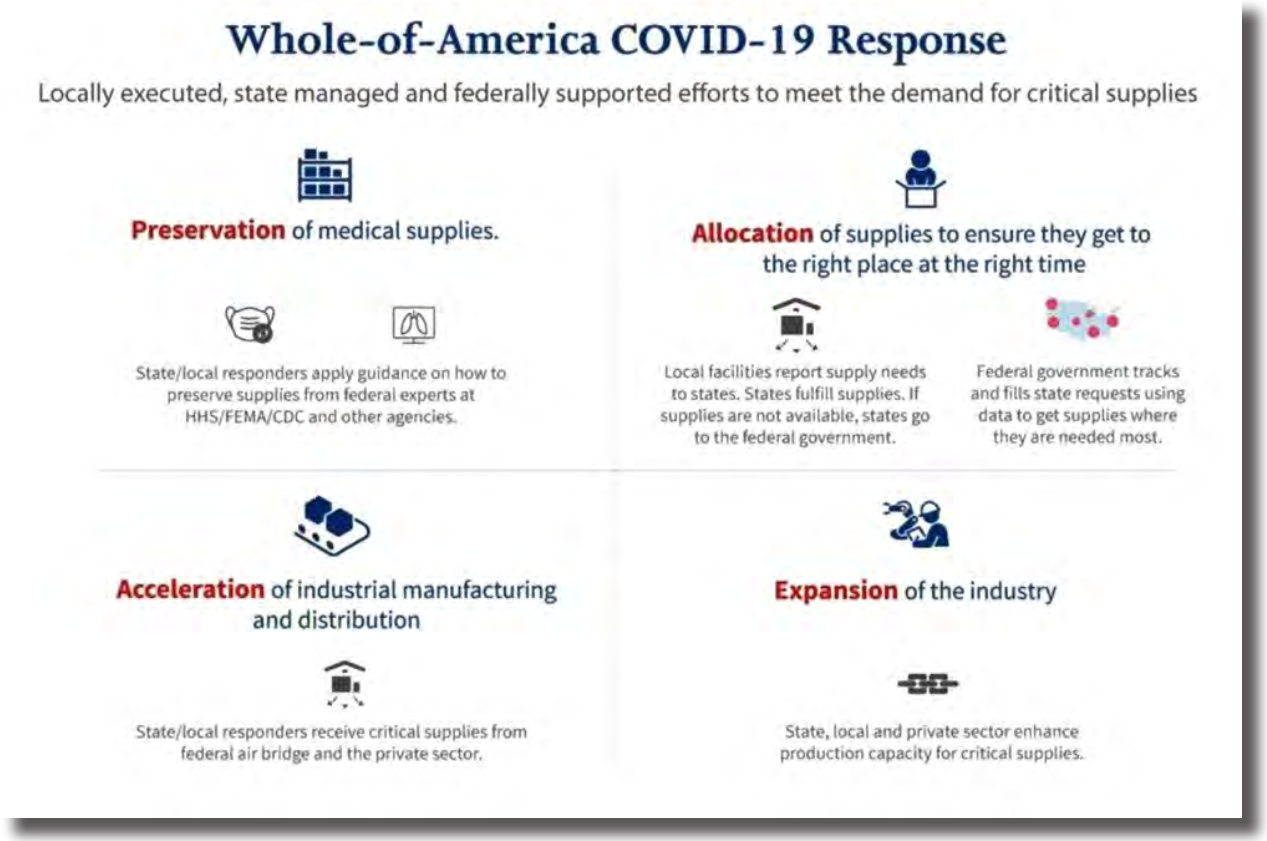
reducing shipment time from weeks to days.[62] This airbridge cut the duration of transporting international shipments down from 37 days on a ship to just one day by air, proving integral to the federal strategy to manage critical shortages of PPE and other medical supplies.

The authority to use the Defense Production Act (DPA) for health and medical resources for COVID-19 was delegated to DHS and HHS in Executive Order 13911, "Delegating Additional Authority under the Defense Production Act with Respect to Health and Medical Resources to Respond to the Spread of COVID-19" (March 27, 2020). The DPA is an authority the President may use to expand the production of supplies and services from the private sector as needed to promote national defense. The Secretary of Homeland Security delegated this authority to FEMA, which FEMA relied on to increase the production and distribution of ventilators, N-95 masks, and medical countermeasures, in coordination with federal partners.

In addition, illicit actors saw an opportunity to exploit legitimate trade lanes to bring counterfeits into the United States due to the COVID-19 crisis. To combat counterfeit

and substandard medical products, CBP focused on seizing test kits, face masks, EPA-prohibited anti-virus lanyards, and prohibited chloroquine that were unsafe for the U.S. public. To accomplish this, CBP engages with partner government agencies such as EPA and FDA to target and interdict high-risk products in these categories. On December 7, 2020, alone, more than 100,000 counterfeit 3M N95 surgical masks intended for use by hospital workers were seized by ICE and CBP, after determining they were counterfeit by working with the National Intellectual Property Rights Coordination Center and 3M Company.[63]

ICE began conducting Operation Stolen Promise in April 2020 to target COVID-19 related fraud. Operation Stolen Promise resulted in 170l arrests, more than $26 million in illicit proceeds seized, 148 search warrants, and more than 1,600 seizures of fraudulent and prohibited material. ICE launched Operation Stolen Promise 2.0, expanding the focus to combat the next wave of anticipated fraud related to the COVID-19 vaccine and other treatments, illustrating the ongoing efforts in keeping the homeland safe and free from corruption. ICE recently seized two fraudulent domain names that purported to be websites of actual biotechnology companies developing treatments for COVID-19 but were in fact set-up to collect the personal information of individuals visiting the sites for nefarious use.[64]



HOMELAND SECURITY ADVISORY COMMITTEE: ECONOMIC SECURITY SUBCOMMITTEE REPORT

The Homeland Security Advisory Committee (HSAC) provides advice and recommendations to the Secretary on matters related to homeland security. The Council comprises leaders from state and local government, first responder communities, the private sector, and academia. In November 2020, the HSAC's Economic Security Subcommittee published its final report on economic security examining both economic security threats and issuing a suite of recommendations, both new and supporting existing efforts.[65] The report's stated principal goal was to address how DHS can contribute to the goal of greater economic security and identify key roles for which the department is best postured to fill if it is not already doing them. In addition to recommending the establishment of a Deputy Assistant Secretary for Economic Security, the report highlighted risks posed by supply chain dependences on China, a significant focus of TES and DHS as a whole. TES strongly supports the findings and recommendations made by the HSAC in their final report especially but not limited to those listed below and looks forward to continuing to implement several of the recommendations within.

Recommendation: "A Deputy Assistant Secretary for Economic Security should be institutionalized within the Office of Strategy, Policy, and Plans."
The establishment of TES and the Office of Economic Security within TES is a direct result of this recommendation and led to the creation of this report and current and forthcoming DHS-led economic security efforts.

Recommendation: "The department should institutionalize the Economic Security Council. Congress should provide a legislative mandate for the establishment and maintenance of the council to identify concentrated risks, to set priorities and to coordinate enterprise-wide action on economic security matters."
TES currently leads the Trade and Economic Security Policy Council which seeks to accomplish this goal. Legislative institutionalization of this Council would further aid in this effort.

Recommendation: "TSA and the Deputy Assistant Secretary for Economic Security should jointly review the threat posed by NucTech and other passenger and cargo screening equipment from China, with particular emphasis on

NucTech's access to data and algorithms used by security agencies. DHS should decide whether the use of insecure equipment is consistent with TSA's foreign airport security assessment standards."

Per this recommendation, TES is working closely in collaboration with DHS Components to review the threat posed by NucTech and other passenger and cargo screening equipment stemming from China. Based on this information, TES found that NucTech's vast market penetration and hostile data practices from China enable China to have access to sensitive cargo and personnel information. This sensitive information provides an intelligence and intellectual property treasure trove for the government of China and TES is working closely with the interagency and Congress to mitigate these risks.

Recommendation: "DHS should engage its interagency partners to:

- **Spur creation of a technology oversight and regulating task force to ensure that rapidly evolving Chinese technology does not evade necessary regulation;**
- **Expand UAS regulatory resources (with support from Congress);**
- **Encourage and actively support innovation in the development and production of UAS in the United States by U.S. companies, particularly for those UAS intended for U.S. government use;**
- **Regulate the export of data (such as imagery) collected by UAS manufacturers;"**

TES's economic security efforts significantly rely upon interagency partners for key information about critical domains. UAS technologies, mitigate risks posed by UAS technologies, and potentially find areas where regulation is necessary. Though these efforts are ongoing, the creation of a technology oversight and regulating task force to accomplish the HSAC's goals for this recommendation has not yet been accomplished. However, creating the task force would strengthen regulation against UAS providers of flawed equipment.

Recommendation: "The intelligence community and DHS should create a joint supply chain intelligence center with private sector entities as participants

and customers. This center should provide practical guidance about suppliers that may pose a particular risk. The center should also influence intelligence collection priorities and provide feedback to improve the quality of supply chain intelligence."

While this recommendation has not yet been adopted, improved collaboration between DHS and the intelligence community would create a filled-in picture of the global economic playing field. Shared situational awareness would enable DHS to collaborate with the private sector and craft proactive policies that strengthen supply chains where risks are identified.

Trade and Economic Security Sub-Office Actions in 2020

The Trade and Economic Security sub-office continuously evaluates risks to critical economic security domains and works to provide solutions to challenges posed by these risks. To do this, it leverages the capabilities of DHS's Components to provide inputs into policy and regulatory proceedings or formulate legislative recommendations. It also coordinates with the White House to draft Executive Orders and Presidential Memorandums and provided policy inputs.

Data Security Business Advisory

In December, TES issued a business advisory for U.S. businesses warning of risks associated with the use of data services and equipment from firms linked to China. Businesses expose themselves and their customers to heightened risk when they share sensitive data with firms located in China, or use equipment and software developed by firms with an ownership nexus in China, or with firms that have Chinese citizens in key leadership and security-focused roles. Due to PRC legal regimes and known PRC data collection practices, this is particularly true for data service providers and data infrastructure.

Report on Combating Trafficking in Counterfeit and Pirated Goods

TES produced for Congress the Report on Combating Trafficking in Counterfeit and Pirated Goods in coordination with Components, the Interagency Executive Steering Committee, and the White House Office of Trade and Manufacturing Policy (OTMP). After the production of this report, TES led several implementation efforts including contributing to legislative efforts, Component-led efforts, and rulemaking proceedings proposed by the report.

Overall Congressional Efforts

TES supported DHS Leadership in their participation in Congressional briefings and committee hearings on a variety of topics, including the Counterfeiting Report, forced labor, supply chain security and more. TES also drafted the congressionally-mandated report, Certain Rail Investments by State-owned or State-controlled Enterprises leveraging inputs from TSA, CISA, I&A, and the U.S. Department of Transportation. ->

LEADERSHIP AND PARTICIPATION IN GOVERNMENT-WIDE EFFORTS

DHS is currently engaged in the following lines of effort to secure U.S. supply chains and counter foreign threats and influence:

EO 13873 ICT Supply Chain Securing the Information and Communications Technology and Services Supply Chain.

Per this Executive Order, DHS provided the Commerce Department with a vulnerability study that assesses the most critical information and communications technologies and services (ICTS) in the information technology and communications sectors. In addition, DHS is working with Commerce and the interagency to develop a risk analytical framework for considering individual matters under this Executive Order.

Information and Communications Technologies Supply Chain Risk Management Task Force.

DHS leads this task force which is developing a common framework for the bi-directional sharing of supply chain risk information between government and industry

Trade and Economic Security Sub-Office Actions in 2020 (Continued)

International Efforts

TES coordinated the review and submission of USG input to the Organisation for Economic Co-operation and Development (OECD) Foreign Trade Zones (FTZ) Recommendation implementation documents. It also provided support to I&A and the Economic Security Mission Center (ESMC) on trade issues and those relating to CFIUS. TES coordinated DHS input into the Synthetics Trafficking and Overdose Prevention (STOP) Act regulations, which require advance electronic data on all imported international mail packages. It also coordinated DHS input into Congressional and GAO STOP Act status reports.

Forced Labor Issues

TES led the establishment of the Forced Labor Enforcement Task Force as required by the USMCA Implementation Act. In addition, it oversaw the development of the DHS report Forced Labor Enforcement Task Force: Establishing Timelines.

Other Security Efforts

TES organized interagency and Intelligence Community participation in the DHS-led Secure Cargo Container Initiative as part of the Department's layered approach to port and container security.

Federal Acquisition Security Council.

DHS is a member of the Federal Acquisition Security Council (FASC) which develops criteria to determine the risk of the ICT supply chain, disseminate supply chain risk information, and decides what action to take to mitigate the risk.

Committee on Foreign Investment in the United States.

To the extent that supply chain risks may arise as a result of foreign investment in U.S. businesses, DHS works with its partners in the interagency as a member of CFIUS to identify and mitigate those risks.

EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom).

Where supply chain risks to U.S. telecommunications networks may arise as a result of foreign persons holding certain licenses to provide telecommunications services in the United States, DHS works with the Departments of Justice and Defense to mitigate those risks.

EO 13920 Securing the United States Bulk-Power System.

Per this Executive Order, DHS supports the Department of Energy in identifying risk information and risk management practices to inform the procurement of energy infrastructure and is coordinating with the Department of Energy and others in the interagency to assist with issuing regulations to secure America's bulk-power system.

Future Prospectus

The U.S. Government has always had an interest in ensuring the security of certain supply chains, working with stakeholders to identify vulnerabilities, and leveraging the federal enterprise to mitigate identified risks. In 2020, the U.S. Government built on those previous efforts, implementing new regulatory and policy measures to more proactively manage risk to economic security. These actions are forward-looking and designed to equip the U.S. Government with the ability to react to newly identified and emerging threats. At the same time, U.S. industries must also elevate supply chain security as they drive innovation and economic growth.

The COVID-19 pandemic presented a "supply chain Sputnik moment" for U.S. stakeholders. Failure to recognize this will make it harder to secure a prosperous, growing, and resilient U.S. economy for future generations. At the very least, this moment should catalyze discussions as to the factors that allowed adversaries to deepen their influence and control of significant segments of critical supply chains. It is also a good time to revisit the level of future government intervention.

The future is uncertain, but malleable. The trade and investment landscape changed, making it imperative that U.S. stakeholders adjust through prioritization of risks to critical economic domains, combined with targeted action to mitigate the most pernicious of those risk. TES was created under the basic premise that U.S. Government must acknowledge and confront a rising China, and that DHS is in an excellent position to address foreign exploitation of supply chains, prevent predatory investment in U.S. and foreign countries, and stop physical and cyber theft of intellectual property and key technology. Some of this work is already underway, and some remains to be set in motion. The focus at this point should be how to achieve a level of intervention that combats foreign aggression while also facilitates U.S. economic growth and technological dominance.

SPECTRUM OF INTERVENTION

U.S. Government intervention to address economic risk can be viewed on a spectrum from no intervention, all the way to state-led capitalism. And since the second order effects of government intervention will likely cascade down to the critical domains

identified herein, it is important to find the right level. The goal of intervention should be to ensure robust and competitive supply from a diverse set of suppliers, both domestic and foreign. To address the particular set of externalities presented by foreign supply, the goal should also be to encourage the adoption and compliance with similar rules, as part of an international system of open markets. In our current environment, that may be difficult, due in part to the damage inflicted on global markets by China and other adversarial nations.

NO INTERVENTION

A future where the U.S. Government takes zero mitigating actions and leaves critical economic domain supply chains solely in the hands of market forces is perhaps the least likely path forward, but also the worst-case scenario. During the prior five years, the U.S. Government made progress in securing greater economic security, through active trade regulatory and enforcement efforts, cyber threat identification and mitigation, public-private partnerships, and work with allies and partners in bilateral and multilateral settings. The lack of these efforts would have led to even more dire conditions and economic uncertainty.

In the face of aggressive and strategic competitors like China, a "no mitigation" scenario will typically lead to a future where U.S. critical economic domains are reliant wholly or in some part on PRC firms that are either legally or illegally funneling U.S. data back to China. These firms could siphon off U.S. intellectual capital and enable China's strategy of civil-military fusion by bolstering PRC companies with illicitly acquired U.S. intellectual property. Billions of dollars would continue to be lost to IP theft and cyber exploitation of vulnerabilities within each domain. U.S. companies would be pushed out of key markets, particularly in telecommunications and manufacturing where PRC companies undercut fair market prices and leverage low labor costs to increase their market penetration. Lack of action would likely lead to increased or sustained PRC investment in critical supply chains lessening the ability for the United States and its allies and partners to combat PRC influence and further deepening dependences.

LIMITED INTERVENTION, ON A TRANSACTION BASIS

Limited intervention represents the status quo where the government provides limited sector-by-sector support. Punitive measures like sanctions and tariffs are applied, but

usually in a highly-targeted manner, and without concurrent incentives and investments to strategically shape private sector behavior. Limited intervention in this way is largely transactional and fails to combine efforts in partnership with the private sector and other stakeholders to create large-scale incentives. By punishing only those companies that get caught, government intervention in this manner can disproportionately impose undue regulatory burdens, altering the competitive landscape in unintended ways. It can also make the government slow to adapt to the private sector, and chase innovation into less restrictive jurisdictions around the world.

This type of limited intervention, on a transaction by transaction basis, has not sufficiently improved U.S. global competitiveness in the face of the evolving threats. While combining such actions with efforts that aim to remove unnecessary regulatory barriers demonstrate the right intentions, they are usually not reciprocated by other governments and in some instances counterproductive. In addition, a narrow transactional approach does not provide an efficient way for the government to invest in certain industries, or research and development. It also limits private sector incentives to identify and mitigate risks from adversaries.

This model for addressing risk fall short in that it only tells industry what not to do, assumes the government can accurately identify risk in every case, and does not provide practical government-enabled solutions that directly promote innovation and competitiveness. This is especially true in areas where U.S. businesses are being pushed out of markets by foreign government assisted efforts, like mobile network infrastructure. Without increased tools to help U.S. companies compete against foreign government assisted conglomerates, the limited, transactional approach will further ossify U.S. innovation, while allowing certain economic vulnerabilities to deepen.

PUBLIC-PRIVATE COLLABORATION FOR INTERVENTION

A collaborative approach, with government and industry working together to identify and mitigate risks is the best way to preserve innovation and build the foundations for economic security. This future represents a proactive strategic approach to risk mitigation that leverages the combined input of the U.S. Government, allies and partners, and the private sector. Identifying not only areas where the United States is losing market share but also areas where the United States has significant market share, but those supply chains might be threatened by current and future adversaries

is important. These combined inputs will help the U.S. Government, allies and partners, and the private sector to identify key current and future technologies in each critical domain that will be instrumental to U.S. economic security in the next several decades and appropriately direct efforts to promote those innovative industries at every step in their supply chains. Unlike the moderate intervention approach, close collaboration across society will ensure that government intervention is strategic and facilitates growth and competition rather than being sporadic and counterproductive. This approach would lessen the likelihood of critical dependences on single nations like China. The U.S. Government would need to expand upon joint efforts with allies and partners to incentivize U.S. and allied countries to diversify their supply chains eliminating critical dependences on sole providers.[66]

Expanding partnerships between the U.S. Government and private industry would also bolster competitiveness of U.S. firms enabling them to offer affordable and high-quality alternatives to allies and partners removing their needs to rely on untrusted vendors. Pairing these partnerships with improved focus on countering PRC strategic investments in critical supply chains would reduce PRC influence and ability to exploit supply chains after they are diversified away from China. In the aggregate, these actions would result in secure and resilient national critical functions like ICT systems, transportation, positional and navigation systems, healthcare and medicine, and power and electricity distribution. Intellectual property like research on new and emerging technologies would be significantly safer from theft or counterfeiting and adversary nations ability to exploit supply chain chokepoints would be reduced. Embracing this approach would enhance not only U.S. economic security and prosperity, but also that of allies and partners benefitting the entire world.

Moderate intervention that uses a "whole-of-society" strategic approach will ensure that the government serves as a helpful facilitator that proactively helps the private sector identify and mitigate risk, incentivizes diverse supply chains, and strengthens U.S. long-term market competitiveness in global markets.

If the emerging regulatory regimes are expanded, such as executive orders and focused regulatory action intended to diversity supply chains and stoke U.S. competitiveness, the result will be resilient U.S. ICT systems, improved data protection from cyber exploitation, and reduced operational risks that affect the security and resilience of

users. Intellectual property theft will be minimized saving the U.S. billions each year. Supply chains for these sectors will begin to be diversified reducing the risk of dependence on and exploitation from China and leave the United States and the rest of the world with alternative sources of supply.

MAXIMUM INTERVENTION, STATE LED CAPITALISM

Maximum intervention, exhibited by state led capitalism, is an economic system wherein a country's government has significant control over the capital, operations, and profits of its businesses. This economic system is common in nations whose principal sources of revenue come from their fuel and energy sectors.[67] In a state capitalist system, governments aim to manipulate market outcomes for their political purpose. However, sustained government control often leads to undue financial and reputational burdens on businesses, and in most cases, stunts long-term economic growth. Corruption drains off capital, as maximum state intervention tends to lead to a government favoring state-owned entities to the detriment of small and medium sized firms.[68] Since large swaths of innovation come first from small and medium sized entities, this level stifles innovation and creates an economic environment wherein a nation is reliant on the success of a few large firms.

For this reason, the United States should resist a move too far in the direction of direct government intervention in U.S. businesses and global markets. A significant reason for sustained U.S. economic prosperity is the role of innovation and the mechanism through which free markets help to allocate capital to the best businesses for investment. A complete shift away from this system would likely have net negative effects.

63. https://www.cbp.gov/newsroom/local-media-release/ice-cbp-seize-more-100000-counterfeit-surgical-masks-intended-hospital
64. https://www.ice.gov/news/releases/ice-investigation-led-seizure-2-fraudulent-websites-purporting-be-biotechnology
65. https://www.dhs.gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf
66. Huawei is often the most affordable option for telecommunications infrastructure due to subsidies from the PRC government paired with hostile market practices and expanded reliance on it multiplies the risk factor for allies and partners and U.S. firms relying on Huawei infrastructure as it becomes increasingly expensive to find alternative providers.
67. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/state-capitalism-and-the-crisis
68. https://www.economist.com/leaders/2012/01/21/the-rise-of-state-capitalism.

Conclusion

The global economy in 2020 was undoubtedly changed by the effects of COVID-19. While it exposed economic security vulnerabilities to U.S. Global Supply Chains, it also marked significant progress in the creation and implementation of emerging regulatory regimes to mitigate risk and prevent more vulnerabilities in the future. Expanding upon current government and DHS efforts to mitigate risk to critical domains is necessary for the long-term economic security of the United States, particularly as adversarial nations like China seek to exploit these vulnerabilities for their own strategic gain. There needs to be greater proactive strategic vision paired with policy measures and investments that not only promote innovation and competitiveness but also ensure supply chains and internet-enabled systems are secure and resilient. The Department of Homeland Security through the Trade and Economic Security sub-office will continue existing efforts to address newly identified issues, gaps in current efforts and mitigate risks to critical domains.

Homeland Security

WITH HONOR AND INTEGRITY, WE WILL SAFEGUARD THE AMERICAN PEOPLE, OUR HOMELAND, AND OUR VALUES

www.dhs.gov