Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

EFFECTIVE RESILIENCE AND NATIONAL STRATEGY:

Lessons From the Pandemic and Requirements for Key Critical Infrastructures

Franklin D. Kramer

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Forward* Defense (*F*D)** helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces ***Forward-looking analyses of the trends, technologies, and concepts that will define the future of warfare, and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, ***F*D** develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition.

The **Global Strategy Initiative** serves to directly advance the Scowcroft Center's core mission by cultivating an ecosystem of strategic thinkers and developing sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Global Strategy Initiative works to revitalize, adapt, and defend a rules-based international system in order to foster another 75 years of peace, prosperity, and freedom.

The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

EFFECTIVE RESILIENCE AND NATIONAL STRATEGY:

Lessons From the Pandemic and Requirements for Key Critical Infrastructures

Franklin D. Kramer

ISBN-13: 978-1-61977-120-8

October 2020

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The coronavirus pandemic has generated enormous health and economic costs to the United States and exposed significant security vulnerabilities, particularly in the cyber and biological arenas. The resilient capabilities of the health, economic, and security sectors have been inadequate to the challenges. American deaths from the pandemic have far exceeded the combined total of lives lost in the conflicts in Korea, Vietnam, Iraq, and Afghanistan. The economy has suffered the greatest reverses since the Great Depression of the 1930s. The long-standing US strategies of overseas engagement and forward defense have had little relevance to a pandemic that is here in the United States affecting individuals, businesses, and governance. While the National Security Strategy identifies combating pandemics and promoting resilience as strategic objectives, the costs from the coronavirus have been far higher than the United States would have expected or should tolerate.

The enormous challenges presented by the virus are reflective of a broader spectrum of resilience risks facing the United States. Since the turn of the century, three converging factors—the ever-increasing reliance on information and communications technology, the globalization of supply chains, and the rise of China as a competitor—have created vulnerabilities that have put the United States at increasing risk. Along with the biological and health risks that the pandemic has exposed, these vulnerabilities call for an expanded focus on resilience as a key element of US strategy.

These are very difficult issues to resolve. A future pandemic or biological attack could generate even higher costs, as could a comparable disruption to the nation through cyberattacks on critical infrastructures such as the electric grid or the telecommunications and information technology sectors. Moreover, challenges to resilience do not only arise from fast-moving events. While the virus is an extraordinarily disruptive factor—metaphorically, akin to a lightning strike that sets off a forest fire in terms of its rapid consequences—it struck a system in the United States in which key areas had been weakened over time. To continue metaphorically, termites had been eating at the house. Among other concerns: the public health sector has been continuously underfunded, software supply chains are highly vulnerable and subject to attack while material supply chains are highly fragile and subject to disruption, and the United States is suffering significant ongoing economic and security harms from the cyber espionage and state-directed economic practices undertaken by China.

The United States has, however, successfully faced daunting challenges before, and can do so again. But to do so, it needs a more effective national strategic approach to resilience, one which creates an operational capacity to prepare for and withstand the disruptive consequences of both prompt and longer-term resilience challenges.

> "The United States … needs … to establish 'effective resilience' as a foundational objective of … national strategy."

To deal with these issues, this report proposes a strategic and operational framework to establish "effective resilience" as a foundational objective of United States national strategy. Effective resilience means the capacity to prepare for and withstand shocks of the magnitude of a major pandemic or equivalent such as a major cyber attack with any resulting disruption significantly less than that caused by COVID-19. Effective resilience also needs to encompass longer-term challenges, including those posed to the economy particularly by Chinese cyber espionage and state-driven economic practices. Achieving effective resilience in the United States should be a fundamental driver of executive and Congressional action that will necessarily be in full partnership with the private sector. The report undertakes a multisector approach focused on key critical infrastructures because lack of resilience in any of these arenas can have cascading consequences resulting in devastating impacts on the nation as a whole. The report further takes a more extensive look at the health sector because of the potential consequences of a future pandemic. Overall, the main conclusion of the report is that it is extremely important to make effective resilience a coherent and comprehensive strategic national objective.

To achieve that goal, the report recommends:

1) a Strategic Framework for Key Critical Infrastructure Resilience, which would include "Resilient Industrial Bases" for key critical infrastructures including a plan for resilience of nationally critical supply chains; establishing "resilience stress tests" for companies in key critical infrastructures; and development and implementation of cybersecurity "resilient architectures" for key critical infrastructures.

2) a Strategic Framework for Health Sector and Biological Resilience, which would include high levels of research and development funding on emerging and infectious diseases including "moonshot" initiatives directed to critical health problems; enhanced support for public health activities to increase the capacity for prevention of and response to pandemics or biological attacks; expanded utilization in the health arena of artificial intelligence through the establishment of trusted data bases available to researchers and analysts; a national plan to respond to a pandemic or biological attack that would be federally-directed pursuant to a new "Stafford Act-plus" legislative mandate; and expanded research and development and planning to enhance resilience to biological attack; and

3) establishment by Congress of a Resilience Commission, with membership incorporating executive, congressional, state, local, private sector, and academic perspectives to undertake factfinding and make recommendations on an ongoing basis regarding the implementation of an effective resilience strategy.[1]

Specific recommendations:

A. Key Critical Infrastructure Resilience

1. The critical infrastructures of defense, energy (electric grid and pipelines), food, finance, health, information and communications technology, transportation, and water ("key critical infrastructures") are of the highest importance to the economy and warrant priority review to assure resilience against both immediate shocks and longer-term challenges. The federal government has designated sector-specific agencies for each of the key critical infrastructure sectors.[2] Each sector-specific agency should undertake—under a Congressional mandate if necessary—a review of the key critical infrastructure sector under its auspices that will lead to the Congressionally approved establishment of an appropriate Resilient Industrial Base for each sector.

2. In undertaking the development of Resilient Industrial Base strategies, each sector-specific agency should determine the capacities required throughout the supply chain to assure availability and integrity of products and services—and the types of incentives and support necessary to achieve those capacities; a process for creation of future capabilities, including support to research and development to ensure resilience will be maintained in the face of emerging and advanced technologies; and the need to evaluate which entities to exclude from, or limit their participation in, the supply chain for the sector—an issue most obviously concerned with China.

3. In the context of establishing a Resilient Industrial Base for a particular sector, it should be generally satisfactory to include allies and reliable partners in the supply chain, much as is done in the Defense Industrial Base. However, the precise contours of what and how much should be maintained in the United States, and how that would be accomplished, will require a granular review by the sector-specific agency and approval by Congress.

4. Perhaps the most important issue for the supply chains for key critical infrastructures is whether and to what degree those supply chains should rely on China. Supply chains have developed globally so the sector-specific agency needs to understand the practicalities, including the costs, of recommending any changes. Nonetheless, there are certain areas where China should be entirely excluded and others where a "China plus one" strategy will be an appropriate approach.

5. For strategic sectors vital to national security or other critical national objectives, Chinese products, components, and services should be excluded from the supply chain unless the use is approved by the US government. That limitation would encompass defense and the intelligence community

6. For sectors not designated strategic for national security reasons, the question of China's exclusion from the supply chains should nonetheless be evaluated at a more granular level. This issue will be of greatest concern in the context of software. Software frequently includes flaws, creating vulnerabilities for exploitations, and supply chains are a mechanism for inserting maliciously intended flaws. Congress should require that the sector-specific agencies prohibit the use of Chinese software in elements of the supply chain that could lead to exploitations posing significant risks.

7. Congress has required under section 3112 of the CARES Act that certain pharmaceutical providers

1 There are additional areas that warrant examination for resilience including: the financial area, natural disasters, and climate change, but those and others are beyond the scope of this analysis. For an example of resilience-based analysis focused on climate adaptation, see Kathy Baughman McLeod, "Building a Resilient Planet: How to Adapt to Climate Change From the Bottom Up," *Foreign Affairs*, May/June 2020, https://www.foreignaffairs.com/articles/2020-04-13/building-resilient-planet.

2 US Department of Homeland Security: Cybersecurity and Infrastructure Security Agency, "Sector-Specific Agencies," 2018, https://www.cisa.gov/sector-specific-agencies.

have a resilience plan.[3] A resilience plan mandate should be expanded to other key critical infrastructures, and Congress should require dual sourcing with the supply chain including a "plus one" country so that China will not be in a sole or dominant position. Specifically, inasmuch as a great deal of medical material and pharmaceuticals are currently produced in China, which cannot be counted on as a reliable source, the United States should, at a minimum, have a "China plus one" approach to sourcing for critical health requirements.

8. Congress should require that resilience stress testing be utilized for the key critical infrastructure sectors and that the sector-specific agencies develop resilience stress tests for their sector. Congress should provide the resources necessary to accomplish the mappings of supply chains, which are costly endeavors but required as part of creating effective resilience stress tests. Congress should require that the sector-specific agencies jointly integrate the results regarding supply chain mappings of companies and sectors into an overall view that gives a basis for an effective national approach.

9. Congress should enact legislation that will make it the policy of the United States to respond to Chinese predatory practices in order to assure long-term resilience of US firms in competitive markets which are unfairly affected by Chinese state-directed economic practices. While the President's authorities are very broad, Congress should review the effectiveness of the current system, including the use of import restraints and/or selective focused tariffs, so as to ensure a level playing field for U.S. firms. Congress should further require the sector-specific agencies to determine whether offsetting actions need to be undertaken to assure the resilience of the key critical infrastructures including their supply chains.

10. The sector-specific agencies should both utilize their existing authorities and recommend to Congress any additional steps to support the innovative capacities of the key critical infrastructure sectors under their jurisdiction, as well as the firms that support them. This will enhance the capacity of the firms to deal with shocks and to remain competitive over the long term.

11. Cybersecurity resilient architectures should be developed and implemented for the key critical infrastructures of energy, finance, food, health, transportation, water, and the defense industrial base, with federal funding to support both the development and operation of such architectures. The information and communications technology sector will be both a recipient and a participant in building cybersecurity resilient architectures.

12. Congress should enact legislation that would establish a framework for a research and development strategy, leading to the creation of resilient architectures that key critical infrastructure providers can rely on. A combined public-private research and development strategy should be utilized for the creation of resilient architectures. This would involve engaging key elements of the federal government, the information and communications technology sector, and the critical infrastructures for whom the architectures would be developed, each of which has relevant expertise.

13. As part of its legislative process, Congress should determine the market arrangements, including legal requirements and financial incentives, that are necessary to encourage the development of an expert sector that would operate cybersecurity resilient architectures on behalf of key critical infrastructures.

14. Congress should authorize and appropriate the costs of operating resilient architectures for designated key critical infrastructure firms to be underwritten by creating a line item in the federal budget. In this way resilience measures would become part of the budget for the Department of Homeland Security (DHS) or, alternatively, in the budgets of the sector-specific agencies.

B. Health Sector and Biodefense Resilience

15. Congress should require the National Institute for Allergy and Infectious Diseases to develop a multiyear research and development program with significantly increased resources for both the public and private sectors, including the development of coordinated public-private partnerships. As part of its legislative process, Congress should receive expert testimony as to appropriate areas of focus, including whether and which health challenges warrant a "moonshot" approach.

16. Congress should establish a substantially increased public health budget including funding levels and other incentives necessary to ensure a satisfactorily sized public health workforce and modernization of state and local public health technology systems.

3 Coronavirus Aid, Relief, and Economic Security Act, Section 3112, "Additional Manufacturer Reporting Requirements In Response To Drug Shortages," https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

17. Congress should request that the National Security Commission on Artificial Intelligence (A/I Commission) recommend a framework to assure the establishment, organization, and usage of data sets for artificial intelligence analysis relevant to the prevention of, preparation for, and response to a pandemic. Data sets can be public, private, or a combination. Further, they should be generated both for research and development, and for operational purposes relevant to responding to a pandemic or biological attack. The A/I Commission should further recommend a research and development program to generate the security capabilities necessary to combine effective data collection and usage with desired privacy requirements.

18. Congress should enact the changes in statutory authorities that would be necessary to create an effective federally directed coordination approach for federal/state/local/critical infrastructure interactions in the context of a nation-wide emergency. This would, in effect, legislate a "Stafford Act-plus" that puts the federal government in charge if a pandemic or comparable event has occurred.

19. Congress should establish a federal framework that provides the necessary technical support and resources to states and localities to ensure the collection and reporting of data relevant to preventing, preparing for, and responding to a pandemic. Congress should enact a framework for an effective and funded testing system that will operate through coordinated federal, state, and local governmental efforts, and engage public and private health entities and providers.

20. Congress should require the establishment of a Joint Interagency Task Force (JIATF) that will undertake the establishment of the necessary operational planning, exercising, and training as part of a national pandemic plan. Congress should also require regular reporting and testimony as to the effectiveness of the JIATF efforts. Given the need for national and local engagement in any effective response, both top-down and bottom-up planning, training, and exercising will be necessary.

21. Congress should require that the federal government undertake to regularize an appropriate level of inventory in the Strategic National Stockpile, ensuring there are sufficient on-hand materials through contracting with manufacturers.

22. Congress should require the establishment of a Health Sector Base as one of the Resilient Industrial Bases.

23. Congress should require a multipart initiative with operational content to enhance biodefense against a potential adversarial attack including: a roadmap for effective biosurveillance programs; Strategic National Stockpile inventory adequacy with respect to pathogens most likely to be utilized in an adversarial attack; a review by the Defense Department leading to greater focus on homeland biodefense including advanced research and development by the Defense Advanced Research Projects Agency and other DOD laboratories; and an operational plan, incorporating the National Guard, to respond to an attack on one or several cities including the requirement for decontamination.

C. Resilience Commission

24. Congress should establish a "Resilience Commission," with membership incorporating executive, congressional, state and local, private sector, and academic perspectives, to undertake factfinding and make recommendations on an ongoing basis regarding the implementation of an "effective resilience" strategy.

I. INTRODUCTION

The coronavirus pandemic has generated enormous health and economic costs to the United States and exposed significant security vulnerabilities, particularly in the cyber and biological arenas. The resilient capabilities of the health, economic, and security sectors have been inadequate to the challenges. American deaths from the pandemic have far exceeded the combined total of lives lost in the conflicts in Korea, Vietnam, Iraq, and Afghanistan. The economy has suffered the greatest reverses since the Great Depression of the 1930s. The long-standing US strategies of overseas engagement and forward defense have had little relevance to a pandemic that is here in the United States affecting individuals, businesses, and governance. While the National Security Strategy identifies combating pandemics and promoting resilience as strategic objectives, the costs from the coronavirus have been far higher than the United States would have expected or should tolerate.

The enormous challenges presented by the virus are reflective of a broader spectrum of resilience risks facing the United States. Since the turn of the century, three converging factors—the ever-increasing reliance on information and communications technology, the globalization of supply chains, and the rise of China as a competitor—have created vulnerabilities that have put the United States at increasing risk. Along with the biological and health risks that the pandemic has exposed, these vulnerabilities call for an expanded focus on resilience as a key element of US strategy.

These are very difficult issues to resolve. A future pandemic or biological attack could generate even higher costs, as could a comparable disruption to the nation through cyberattacks on critical infrastructures such as the electric grid or the telecommunications and information technology sectors. Moreover, challenges to resilience do not only arise from fast-moving events. While the virus is an extraordinarily disruptive factor—metaphorically, akin to a lightning strike that sets off a forest fire in terms of its rapid consequences—it struck a system in the United States in which key areas had been weakened over time. To continue metaphorically, termites had been eating at the house. Among other concerns: the public health sector has been continuously underfunded, software supply chains are highly vulnerable and subject to attack while material supply chains are highly fragile and subject to disruption, and the United States is suffering significant ongoing economic and security harms from the cyber espionage and state-directed economic practices undertaken by China.

The United States has, however, successfully faced daunting challenges before, and can do so again. But to do so, it needs a more effective national strategic approach to resilience, one which creates an operational capacity to prepare for and withstand the disruptive consequences of both prompt and longer-term resilience challenges.

> "Achieving effective resilience … should be a fundamental driver of executive and Congressional action."

To deal with these issues, this report proposes a strategic and operational framework to establish "effective resilience" as a foundational objective of United States national strategy. Effective resilience means the capacity to prepare for and withstand shocks of the magnitude of a major pandemic or equivalent such as a major cyber attack with any resulting disruption significantly less than that caused by COVID-19. Effective resilience also needs to encompass longer-term challenges, including those posed to the economy particularly by Chinese cyber espionage and state-driven economic practices. Achieving effective resilience in the United States should be a fundamental driver of executive and Congressional action that will necessarily be in full partnership with the private sector. The report undertakes a multisector approach focused on key critical infrastructures because lack of resilience in any of these arenas can have cascading consequences resulting in devastating impacts on the nation as a whole. The report further takes a more extensive look at the health sector because of the potential consequences of a future pandemic. Overall, the main conclusion of the report is that it is extremely important to make effective resilience a coherent and comprehensive strategic national objective.

To achieve that goal, the report recommends:

1) a Strategic Framework for Key Critical Infrastructure Resilience, which would include "Resilient Industrial Bases" for key critical infrastructures including a plan for resilience of nationally critical supply chains; establishing "resilience stress tests" for companies in key critical infrastructures; and development and implementation of cybersecurity "resilient architectures" for key critical infrastructures.

2) a Strategic Framework for Health Sector and Biological Resilience, which would include high levels of research and development funding on emerging and infectious diseases including "moonshot" initiatives directed to critical health problems; enhanced support for public health activities to increase the capacity for prevention of and response to pandemics or biological attacks; expanded utilization in the health arena of artificial intelligence through the establishment of trusted data bases available to researchers and analysts; a national plan to respond to a pandemic or biological attack that would be federally-directed pursuant to a new "Stafford Act-plus" legislative mandate; and expanded research and development and planning to enhance resilience to biological attack; and

3) establishment by Congress of a Resilience Commission, with membership incorporating executive, congressional, state, local, private sector, and academic perspectives to undertake factfinding and make recommendations on an ongoing basis regarding the implementation of an effective resilience strategy.[4]

4 There are additional areas that warrant examination for resilience including: the financial area, natural disasters, and climate change, but those and others are beyond the scope of this analysis. For an example of resilience-based analysis focused on climate adaptation, see Kathy Baughman McLeod, "Building a Resilient Planet: How to Adapt to Climate Change From the Bottom Up," *Foreign Affairs*, May/June 2020, https://www.foreignaffairs.com/articles/2020-04-13/building-resilient-planet.

II. LESSONS FROM THE PANDEMIC—UNDERPRIORITIZING RESILIENCE

The challenges the United States has faced in dealing with the coronavirus offer a cautionary tale of the consequences of underprioritizing resilience.

A key cause of inadequate resilience to the coronavirus was a failure to take sufficient steps in the face of earlier warnings about the potential for a pandemic. There were no strategic warnings about this virus specifically, but there were multiple warnings about the dangers of a pandemic and the need to establish stronger safeguards. The warnings date back at least to 1994, when public health expert Laurie Garrett published her best seller, "The Coming Plague." Subsequent to 1994, significant disease outbreaks including Ebola, SARS, and H1N1 underscored expert concerns, but did not receive sufficient responses. Thus:

> "In reporting on the Ebola virus epidemic of 2015, Garrett found that little progress had been made in 20 years: 'The global response to the rise of new pathogens has continued to be limited, uncoordinated, and dysfunctional.'"[5]

Garrett has been far from alone in seeking to raise the alarm. Michael T. Osterholm had similarly underscored the dangers in "Preparing for the Next Pandemic," written in 2005.[6] As Osterholm recently pointed out, "The public health community has for years known with certainty that another major pandemic was on the way, and then another one after that—not if but when…"[7]

The warnings were not limited to subject matter experts. The Bipartisan Commission on Biodefense, chaired by former Senator Joe Lieberman and former Governor Tom Ridge, likewise concluded:

> "The United States is underprepared for biological threats. Nation states and unaffiliated terrorists (via biological terrorism) and nature itself (via emerging and reemerging infectious diseases) threaten us. While biological events may be inevitable, their level of impact on our country is not…Despite significant progress on several fronts, the Nation is dangerously vulnerable to a biological event."[8]

The federal government's 2018 National Biodefense Strategy similarly assessed:

> "Biological threats—whether naturally occurring, accidental, or deliberate in origin—are among the most serious threats facing the United States and the international community. Outbreaks of disease can cause catastrophic harm to the United States…Natural or accidental outbreaks, as well as deliberate attacks, can originate in one country and spread to many others, with potentially far-reaching international consequences."[9]

Quite presciently, the Director of National Intelligence's Worldwide Threat Assessment for 2019 stated:

> "We assess that the United States and the world will remain vulnerable to the next flu pandemic or largescale outbreak of a contagious disease that could lead to massive rates of death and disability, severely affect the world economy, strain international resources, and increase calls on the United States for support. Although the international community has made tenuous improvements to global health security, these gains may be inadequate to address the challenge of what we anticipate will be more frequent outbreaks of infectious diseases."[10]

5 Frank Bruni, "She Predicted the Coronavirus. What Does She Foresee Next?" *New York Times*, May 2, 2020, https://www.nytimes.com/2020/05/02/opinion/sunday/coronavirus-prediction-laurie-garrett.html?referring Source=articleShare.

6 Michael T. Osterholm, "Preparing for the Next Pandemic," *Foreign Affairs*, July/August 2005, https://www.foreignaffairs.com/articles/2005-07-01/preparing-next-pandemic.

7 Michael T. Osterholm and Mark Olshaker, "Chronicle of a Pandemic Foretold," *Foreign Affairs*, July/August 2020, https://www.foreignaffairs.com/articles/united-states/2020-05-21/coronavirus-chronicle-pandemic-foretold.

8 Bipartisan Report of the Blue Ribbon Study Panel On Biodefense, *A National Blueprint for Biodefense*, October 2015," iv, https://biodefensecommission.org/wp-content/uploads/2015/10/NationalBluePrintNov2018-03.pdf.

9 The White House, *National Biodefense Strategy*, 2018, i, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf.

10 Director of National Intelligence, *Worldwide Threat Assessment*, January 2019, 21, https://www.dni.gov/files/ ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Federal government actions were not limited to description and analysis;[11] the warnings generated multiple responses. As Senator Lamar Alexander recently described:

> "During the past 20 years, four Presidents and several Congresses enacted nine significant laws to help local, state, and federal governments, as well as hospitals and health care providers, to prepare for a public health emergency, including a pandemic."[12]

Among other actions, Congress enacted the Public Health Improvement Act (2000), the Public Health Security and Bioterrorism Preparedness and Response Act (2002), the Project BioShield Act (2004), the Public Readiness and Emergency Preparedness Act (2005), the Pandemic and All-Hazards Preparedness Act (2006), the Pandemic and All-Hazards Preparedness Reauthorization Act (2013), the 21st Century Cures Act (2016), and the Pandemic and All-Hazards Preparedness and Advancing Innovation Act (2019).[13]

In sum, the strategic warning was clear enough, and, to some extent, heeded as the passage of multiple enactments indicates. As with other comparable historical failures such as Pearl Harbor and September 11, however, it is not that those in a position to do something deliberately refused action. Rather, they—both governmental and non-governmental actors—took steps, but their main efforts were directed toward what they considered more pressing matters. Ultimately, their ranking of the danger/risk calculus—at least implicitly—saw the pandemic threat as not of the highest consequence.[14]

In the United States over the past decade and more, the concerns receiving greater attention included responding to the financial crisis, enacting tax cuts, reducing regulations, increasing the defense budget, and dealing with Afghanistan, Iraq, and counter-terrorism. The National Security Strategy highlighted "great power competition" especially focusing on Russia and China.[15]

Internationally, the consequences of a pandemic and steps to prevent one were not the grist of heads of state meetings, whether bilateral, at the G-7 or G-20, at the United Nations, or elsewhere. Steps were taken, such as the creation of the Global Preparedness Monitoring Board in 2018,[16] but concerns over pandemics were not on the central agenda.

The private sector as well remained focused on other matters, with the dominant concept being increasing shareholder value. Corporate risk calculations did not prioritize pandemic concerns. As a report from DHS stated:

> "Eighty-five percent of critical infrastructure resources reside in the private sector, which generally lacks individual and system-wide business continuity plans specifically for catastrophic health emergencies such as pandemic influenza. Many businesses have extensive contingency plans in response to threats from diverse natural and man-made disasters. While useful for their intended purpose, these plans may prove ineffective given they do not account for the extreme health impact assumptions and containment strategies projected for a severe pandemic influenza."[17]

To be sure, individuals and governments were not entirely oblivious. With philanthropic and governmental support, the Coalition for Epidemic Preparedness Innovations (CEPI) was established. CEPI is a "global partnership between public, private, philanthropic, and civil society organizations launched in Davos in 2017 to develop vaccines to stop future epidemics…[and whose] mission is to accelerate the development of vaccines against emerging infectious diseases and enable equitable access to these vaccines for people during outbreaks."[18]

11 There were, however, a great many reports: "Congress received many reports from presidential administrations, Offices of Inspectors General, the Government Accountability Office, and outside experts throughout those 20 years warning that the U.S. needed to address the following issues: better methods to quickly develop tests, treatments, and vaccines and scale up manufacturing capacity; better systems to quickly identify emerging infectious diseases; more training for health care and public health workforce; better distribution of medical supplies; and better systems to share information within and among states, and between states and the federal government. Many reports also warned that while states play the lead role in a public health response, many faced workforce shortages and training needs, inadequate stockpiles, and funding challenges. In some instances, overreliance on inflexible federal funding contributed to these problems." Senator Lamar Alexander, *Preparing for the Next Pandemic*, June 9, 2020, 1, https://www.alexander.senate.gov/public/_cache/files/0b0ca611-05c0-4555-97a1-5dfd3fa2efa4/preparing-for-the-next-pandemic.pdf.

12 Ibid.

13 Ibid., 6-13.

14 See the discussion in Christopher Kirchhoff, "Ebola Should Have Immunized the United States to the Coronavirus," *Foreign Affairs*, March 28, 2020, https://www.foreignaffairs.com/articles/2020-03-28/ebola-should-have-immunized-united-states-coronavirus, and "Partly False Claim: Trump Fired Entire Pandemic Response Team in 2018," *Reuters*, March 25, 2020, https://www.reuters.com/article/uk-factcheck-trump-fired-pandemic-team/partly-false-claim-trump-fired-pandemic-response-team-in-2018-idUSKBN21C32M.

15 The White House, *National Security Strategy of the United States of America*, December 2017, 27, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

16 "About Us," Global Preparedness Monitoring Board, https://apps.who.int/gpmb/about.html.

17 Department of Homeland Security, *Pandemic Influenza Preparedness, Response, and Recovery Guide For Critical Infrastructure and Key Resources*, September 19, 2006, ii, https://www.dhs.gov/sites/default/files/publications/cikrpandemicinfluenzaguide.pdf.

18 "Our Mission," Coalition for Epidemic Preparedness Innovations, https://cepi.net/about/whyweexist/.

Twenty years earlier, "GAVI, the Vaccine Alliance" had been created. "[T]he Bill and Melinda Gates Foundation and a group of founding partners brought to life an elegant solution to encourage manufacturers to lower vaccine prices for the poorest countries in return for long-term, high-volume and predictable demand from those countries. In 2000, that breakthrough idea became the Global Alliance for Vaccines and Immunization—today Gavi, the Vaccine Alliance."[19]

In sum, it would be inaccurate to suggest that decision-makers were deliberately acting badly by refusing to take steps to prevent and/or respond to a pandemic. Rather, when it came to taking decisive action, the then-deemed "urgent" crowded out what turned out to be the "important," such as the potential steps that might have made a consequential difference over the course of this pandemic. "Too little, too late" is perhaps a fair summation.

> "The critical issue for policymakers is to … create robust capabilities backed by sufficient resources … Underprioritizing is not an effective strategy."

Going forward, the critical issue for policymakers is to ensure that efforts to shore up resilience ultimately create robust operational capabilities backed by sufficient resources, able to withstand shocks of a magnitude of a major pandemic or comparable national emergency, and to deal with longer-term challenges. Underprioritizing is not an effective strategy.

19 "History," GAVI, the Vaccine Alliance, https://www.gavi.org/our-alliance/about.

III. RESILIENCE CHALLENGES TO KEY CRITICAL INFRASTRUCTURES

The challenges to resilience are, broadly speaking, a consequence of globalization. As many have pointed out, the oceans no longer adequately protect the United States. The September 11 attacks and the establishment of the DHS are testament to both the increased vulnerability and an enhanced response. The Department of Homeland Security's efforts against terrorism have been part of a larger interagency structure—including the Department of Defense and the intelligence community—that has limited attacks in the United States. However, no similar success can be claimed concerning cyber, supply chain, or health/biological vulnerabilities, nor has China been deterred. Each of these factors has undermined the resilience of the United States.

A. Cyber Vulnerabilities in the Information Age

Cyber vulnerabilities, while long-detailed, have been underscored by recent government reports describing the multiple attacks against the health sector, including against companies seeking to develop a vaccine. The seriousness of the problem was highlighted by DHS and the Federal Bureau of Investigation (FBI) issuing a joint alert "warning organizations researching COVID-19 of likely targeting and attempted network compromise by the People's Republic of China (PRC). Healthcare, pharmaceutical, and research sectors working on the COVID-19 response should all be aware they are the prime targets of this activity and take the necessary steps to protect their systems."[20] The DHS and FBI concluded, "China's efforts to target these sectors pose a significant threat to our nation's response to COVID-19."[21] Similarly, in a report endorsed by the United States, the United Kingdom (UK) and Canada identified Russian hackers as "target[ing] various organizations involved in COVID-19 vaccine development in Canada, the United States, and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines."[22]

Such attacks reflect a wider cyber vulnerability. A recent report found, "The state of security in the software supply chain is inadequate and, in some critical respects, getting worse."[23] Thus:

> "With software come security flaws and a long tail of updates from vendors and maintainers. Unlike a physical system that is little modified once it has left the factory, software is subject to continual revision through updates and patches. This makes the supply for code long and subject to myriad flaws, both unintentional and malicious. The private sector's aggregated risk from software supply chain compromises continues to grow. Ever more feature-rich software is finding its way into a widening array of consumer products and enterprise services, enlarging the potential attack surface."[24]

Those vulnerabilities provide an environment susceptible to attack, and adversaries are taking full advantage. As described by the US Director of National Intelligence:

> "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners. China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure."[25]

The Cybersecurity Solarium Commission likewise concluded:

> "For over 20 years, nation-states and non-state actors have used cyberspace to subvert American power, American security, and the American way of life…Chinese cyber operators stole hundreds of billions of dollars in intellectual property to accelerate China's military and economic rise

20 *Chinese Malicious Cyber Activity*, Cybersecurity and Infrastructure Security Agency, May 13, 2020, https://www.us-cert.gov/china.

21 Ibid.

22 "Advisory: APT29 targets COVID-19 vaccine development," National Cyber Security Centre, July 16, 2020, https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development.

23 Trey Herr, June Lee, William Loomis, and Stewart Scott, *BREAKING TRUST: Shades of Crisis Across an Insecure Software Supply Chain*, *Atlantic Council*, July 2020, 6, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf.

24 Ibid., 2.

25 Director of National Intelligence, *Worldwide Threat Assessment*, 5.

and undermine US military dominance. Russian operators and their proxies damaged public trust in the integrity of American elections and democratic institutions. China, Russia, Iran, and North Korea all probed US critical infrastructure with impunity. Criminals leveraged globally connected networks to steal assets from individuals, companies, and governments. Extremist groups used these networks to raise funds and recruit followers, increasing transnational threats and insecurity."[26]

B. Supply Chain Vulnerability in a Global Economy

An immediate impact of the virus has been the disruption of supply chains, not only in the health sector, but in many other sectors as well. That disruption occurred in significant part because many supply chains had been globalized in a "just-in-time" approach on the apparent assumption that a consequential disruption of trade simply would not occur. As one analysis concluded:

> "A major reason for the shortages that have occurred during the pandemic is the lean global supply chains that have been deployed widely in order to reduce costs through efficient allocation of production to low-cost regions; just-in-time methodologies in manufacturing; and holding lower levels of inventory throughout the supply chain. These strategies rely on forecasting based on historical data and do not typically consider any major disruptions."[27]

An analysis from the World Economic Forum stated:

> "The COVID-19 pandemic has hit global trade and investment at an unprecedented speed and scale. Multinational companies faced an initial supply shock, then a demand shock as more and more countries ordered people to stay at home. Governments, businesses, and individual consumers suddenly struggled to procure basic products and materials, and were forced to confront the fragility of the modern supply chain. The urgent need to design smarter, stronger, and more diverse supply chains has been one of the main lessons of this crisis."[28]

However, the problems of creating resilient supply chains go beyond the direct impact from the virus. Globalization has led "many sectors [to] continue to move critical capabilities offshore in pursuit of competitive pricing and access to foreign markets."[29] While that in and of itself does not generate fragility, a government report focused on "Manufacturing and Defense Industrial Base and Supply Chain Resilience" described:

> "a set of … risk[s] … with discrete impacts on America's manufacturing and defense industrial base. These include the rise of single and sole-source suppliers which create individual points of failure within the industrial base, as well as fragile suppliers near bankruptcy and entire industries near domestic extinction. Due to erosion that has already occurred, some manufacturing capabilities can only be procured from foreign suppliers, many of which are not domiciled in allied and partner nations. The concomitant gaps in US-based human capital and erosion of domestic infrastructure further exacerbates the challenge. Ultimately, these negative impacts have the potential to result in limited capabilities, insecurity of supply, lack of [research and development], program delays, and an inability to surge in times of crisis."[30]

In its report published in March 2020, the Congressionally-established Cyberspace Solarium Commission found comparable concerns in the context of the information and communications technology sector, highlighting the need to "address areas where the lack of domestic or trusted industrial capacity itself constitutes a national security and economic security risk."[31] The commission found:

> "Of particular importance, as technology supply chains become more complex and global, the United States has developed a growing dependence on suppliers that may come under malign influence, introducing vulnerability into the ecosystem. To better manage these risks, the United States should develop a more robust capacity to identify and protect against untrusted suppliers

26 "Executive Summary," Cyberspace Solarium Commission, March 2020, 1, https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

27 David Simchi-Levi and Edith Simchi-Levi, "We Need a Stress Test for Critical Supply Chains," *Harvard Business Review*, April 28, 2020.

28 Jesse Lin and Christian Lang, "Here's How Global Supply Chains Will Change After COVID-19," World Economic Forum, May 6, 2020, https://www.weforum.org/agenda/2020/05/this-is-what-global-supply-chains-will-look-like-after-covid-19/.

29 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, 3, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

30 Ibid., p.8.

31 *Cyberspace Solarium Commission*, March 2020, 88, https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

while ensuring the presence of viable alternative suppliers for critical technologies through strategic investment."[32]

C. China Challenges in an Era of Great Power Competition

China presents a series of resilience challenges for the United States.

First, Chinese companies are pervasively present in United States supply chains**.** As the DOD/interagency supply chain task force, noted above, described:

> "In addition to China dominating many material sectors at the upstream source of supply (e.g. mining), it is increasingly dominating downstream value-added materials processing and associated manufacturing supply chains, both in China and increasingly in other countries. Areas of concern to America's manufacturing and defense industrial base include a growing number of widely used and specialized metals, alloys, and other materials, including rare earths and permanent magnets."[33]

> "China presents a series of resilience challenges … [including] whether it will remain a reliable supplier."

Second, that pervasiveness raises the issue of whether China will remain a reliable supplier, particularly when there are political or other pressures such as can occur during a pandemic. Historically, in order to achieve its geopolitical goals, China has utilized economic pressure including restricting supply chains. An example of China's quick turn to economic coercion is the Chinese reaction to a single tweet by the general manager of the Houston Rockets supporting the Hong Kong protesters:

> "[T]he Chinese Basketball Association announced it would sever ties with the Rockets, as did Tencent, the NBA's rights holder in China, and the Rockets' Chinese sponsors…[and] the sports arm of Chinese state broadcaster CCTV announced it would not broadcast the NBA's preseason games being played in China."[34]

The use of such economic coercion is regularly undertaken by China, namely by:

> "Punish[ing] countries that undermine its territorial claims and foreign policy goals with measures such as restricting trade, encouraging popular boycotts, and cutting off tourism."[35]

A detailed list of specific instances of economic coercion would include:

> "(1) Chinese restrictions on rare earths exports and other measures directed at Japan after a collision between a Chinese fishing boat and a Japanese coast guard ship near the disputed Senkaku/Diaoyu islands in 2010; (2) Chinese restrictions on imports of Norwegian salmon after Liu [Xiaobo] won the Nobel Peace Prize in 2010; (3) Chinese reductions of imports of bananas and other agricultural goods from the Philippines as well as cuts in tourism from China after a dispute over the South China Sea from 2012 to 2016; (4) Chinese reductions in tourism and other measures against Taiwan in response to the election of Tsai [Ing-wen] in 2016; (5) Chinese tourism reductions and restrictions on certain trade with South Korea after Seoul agreed to deploy a US THAAD missile defense system in 2016; and (6) temporary Chinese restrictions on cross-border trade with Mongolia after it allowed the Dalai Lama's visit in 2016."[36]

Third, China's involvement in information technology supply chains raises the issue of system and component vulnerabilities, and the potential for the introduction of malware. Those considerations, as noted above by the Cyberspace Solarium Commission, are specifically presented by China's role in 5G technology:

> "First, vendors such as Huawei [Technologies Co., Ltd.] generally have access to the networks for which they provide key elements. That implies they can, with sufficient capability, intercept

32 Ibid.

33 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, 36-37, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

34 Franklin D. Kramer, *Managed Competition: Meeting China's Challenge in a Multi-vector World*, *Atlantic Council*, December 2019, 23, https://www.atlanticcouncil.org/wp-content/uploads/2019/12/Meeting-Chinas-Challenges-Report-WEB.pdf.

35 Peter Harrell, Elizabeth Rosenberg, and Edoardo Saravalle, *China's Use of Coercive Economic Measures, Center for a New American Security*, June 2018, 2, https://s3.amazonaws.com/files.cnas.org/documents/China_Use_FINAL-1.pdf?mtime=20180604161240.

36 Ibid.,7-8; Kramer, *Managed Competition* 23.

> signals running on the networks. Second, the software and/or components may have vulnerabilities by design or by lack of good engineering that can be exploited. Since vendors have access to the networks, inserting vulnerabilities at a later date is also a possibility. Third, the networks could be significantly disrupted by a vendor with access. All these issues have been raised in connection with Huawei."[37]

Fourth is the issue of the impact on market competition from unfair practices undertaken by China's state-driven economic model. This question arises most importantly with respect to advanced and emerging technologies which will be the leading drivers of the global economy. Democratic free market nations do have the innovative capability to develop capabilities in a host of advanced technologies including artificial intelligence, genomics and biological research, quantum computing, nanotechnology, robotics, energy, and information technology.[38] The issue is less innovation than it is the ability to have a fair and efficient market for companies in the face of China's unfair market practices including use of subsidies, commercial cyber espionage, protection of its own market, and forced technology transfers.

The US Trade Representative reports to Congress have described these practices in detail,[39] which can be summarized:

> "In an attempt to dominate critical global markets and manufacturing industries, China leverages policy tools such as low interest loans; subsidized utility rates; lax environmental, health, and safety standards; and dumping to boost its industry. China also uses counterfeiting and piracy, illegal export subsidies, and overcapacity to depress world prices and push rivals out of the global market. It has implemented these tactics to capture much of the world's solar and steel industries and intends to extend its dominance to other industries such as automobiles and robotics."[40]

The impact of China's state-directed economy has been widely discussed and remains a leading policy issue for both the United States and the European Union (EU). As one analysis has described:

> "[W]hile the United States has no reason to fear a fair competition, the "distortive effects" identified by the European Commission, as well as others, significantly affect both future innovation competition as well as the operation of markets more generally. Most importantly, there are critical aspects of China's economy that are systemically incompatible with the Western free market approach. First, the significant differences begin with the [Communist Party of China] CPC and governmental structure and control over markets and enterprises…Second, subsidies are a critical element of the competitive problem…Third, China maintains significant non-tariff barriers to foreign investment and commerce…Fourth, China utilizes multiple methods resulting in "forcible transfer of technology,"…Fifth, and outside of China, another key issue has been Chinese foreign direct investment focused on Western companies with sensitive security-related technologies."[41]

An illustrative example of the consequences of these practices by China is that Huawei undercut Ericsson's bid in the Dutch market for 5G networks by more than 50 percent.[42] The impact of subsidization is reflected in such pricing and will likewise remain an issue in the future. The European Union has recently put this question on its agenda with China.[43] How the United States and the European Union decide what framework to utilize in response to Chinese actions, and the actual implementation of any framework, will determine the future resilience of free markets.

D. Health Sector Vulnerabilities Affecting Resilience

The problems of resilience are notably present in the health sector, as the impact of the coronavirus has demonstrated.

37 Kramer, *Managed Competition*, 21.

38 See Franklin D. Kramer and James A. Wrightson, Jr., *Innovation, Leadership and National Security*, *Atlantic Council*, April 2016, https://www.atlanticcouncil.org/wp-content/uploads/2016/04/Innovation_Leadership_and_National_Security_web_0411.pdf

39 United States Trade Representative, "2018 Report to Congress On China's WTO Compliance," February 2019, https://ustr.gov/sites/default/files/2018-USTR-Report-to-Congress-on-China%27s-WTO-Compliance.pdf.

40 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, 36, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

41 Kramer, *Managed Competition,* 12-14.

42 Pamella Lim and Melissa Goh, "Affordability and 5G Race are Reasons Why Malaysia Continues to Support Huawei, Says Telco Regulator," Channel News Asia, June 27, 2019, https://www.channelnewsasia.com/news/business/huawei-5g-malaysia-support-mcmc-mahathir-11665232.

43 European Commission, Statement by President von der Leyen at the Joint Press Conference with President Michel, Following the EU-China Summit Videoconference, June 22, 2020, https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1162.

1) An Underfunded Public Health System

In the United States, the virus attacked a country that has significantly underfunded its public health systems. This in turn has caused detrimental consequences at the state, local, and federal levels. For states and localities:

> "Federal funding is the backbone of the nation's public health system, and, because so much local public health activity is dependent on funding from state or federal sources, budget cuts at those levels have a trickle-down effect on local communities."[44]

Because of that dependency, "Lack of investment has led to a dangerously underfunded public health infrastructure."[45] The degree of underfunding is substantial: "The Public Health Leadership Forum estimates that an annual infusion of $4.5 billion is needed to fully support core public health foundational capabilities at the state, territory, local, and tribal levels nationwide."[46]

Federal funding to states and localities for public health is generally undertaken through the Centers for Disease Control and Prevention (CDC). However:

> "The lack of core CDC funding to states and localities have made them more vulnerable when an emergency situation occurs, such as the Ebola and Zika outbreaks and, most recently, the novel coronavirus pandemic. While Congress passed essential, specialized, short-term supplemental funding for these outbreaks, temporary measures cannot substitute for the necessary core funding of public health."[47]

One core issue is funding for personnel: "Without day-in, day-out skilled staff and other resources, it isn't possible to ensure the protection of the American public from such threats. Health departments cannot quickly hire and retain experts with the necessary skills and experience with short-term funding."[48]

Inadequate funding has resulted in significant public health workforce issues: "Between 2016 and 2019, the number of state full-time or equivalent people working in public health shrank from 98,877 to 91,540. What's more, burnout is a growing issue, as public health professionals are continually asked to do more with less. The Public Health Workforce Interests and Needs Survey found that a large proportion of workers are considering leaving their organization in the next year, in part due to inadequate pay. Also of concern, state health officials estimate that 25 percent of their workforce will be eligible for retirement this year (2020)."[49]

2) Lack of an Operationally Adequate Federal Framework

The issues at the federal level are similarly difficult, arising at the operational level. There is an ostensible framework. After the September 11 terrorist attacks led to the establishment of the Department of Homeland Security, DHS created the National Response Framework (NRF). The NRF, "provides foundational emergency management doctrine for how the nation responds to all types of incidents."[50] Further, Emergency Support Function (ESF) #8—Public Health and Medical Services Annex is intended to provide a specific framework for health emergencies.[51] The Department of Health and Human Services (HHS) has the lead for health emergencies, and has established an HHS Concept of Operations for ESF #8.[52] A Pandemic Influenza Plan, which was established in 2005 and updated most recently in 2017,[53] states that "the capacity and capabilities developed for pandemic influenza preparedness will enable HHS to respond more effectively to other emerging infectious diseases."[54]

44 *The Impact of Chronic Underfunding on America's Public Health System: Trends, Risks, and Recommendations*, Trust for America's Health, 2020, 22, https://www.tfah.org/wp-content/uploads/2020/04/TFAH2020PublicHealth Funding.pdf.

45 Ibid., 8.

46 Ibid., 8; Public Health Leadership Forum, *Developing a Financing System to Support Public Health Infrastructure*, 2018, 1, https://www.resolve.ngo/docs/phlf_developingafinancingsystemtosupportpublichealth6368694396886 63025.pdf.

47 *Impact of Chronic Underfunding*, 8.

48 Ibid., 17.

49 Ibid., p.7; Kyle Bogaert, MPH, et al., "The Public Health Workforce Interests and Needs Survey (PH WINS 2017): An Expanded Perspective on the State Health Agency Workforce," *Journal of Public Health Management and Practice*, March/April 2019, 16-25, https://journals.lww.com/jphmp/fulltext/2019/03001/the_public_health_workforce_interests_and_needs.6.aspx.

50 US Department of Homeland Security, *National Response Framework Fourth Edition*, October 28, 2019, ii, https://www.fema.gov/media-library-data/1582825590194-2f000855d442fc3c9f18547d1468990d/NRF_ FINALApproved_508_2011028v1040.pdf.

51 US Department of Homeland Security, *National Response Framework, Emergency Support Function #8 – Public Health and Medical Services Annex*, https://www.fema.gov/media-library-data/20130726-1825-25045-8027/emergency_support_function_8_public_health___medical_services_annex_2008.pdf.

52 Department of Health and Human Services, *HHS Concept of Operations for ESF #8*, https://www.phe.gov/Preparedness/planning/mscc/handbook/chapter7/Pages/hhsconcept.aspx.

53 Department of Health and Human Services, *Pandemic Influenza Plan, 2017 Update*, https://www.cdc.gov/flu/pandemic-resources/pdf/pan-flu-report-2017v2.pdf.

54 Id., 3.

In dealing with the coronavirus, however, the actions of the federal government have been essentially ad hoc rather than structured around the purported framework. As one analysis stated, "it was no longer the process that had been planned and exercised."[55] That failure of process has led to multiple issues in dealing with state and local governments, the private sector, and individual citizens.

"In dealing with the coronavirus … the actions of the federal government have been essentially ad hoc rather than structured around the purported framework."

In short, despite the sensible paper documents, the Department of Health and Human Services and its subordinate agencies simply were not ready for the problem of the coronavirus. Initially, HHS did not recognize the degree of the threat the virus presented when it first emerged in China, stating in late January that the "risk to the American public remains low at this time."[56] Even as late as mid-February, HHS described the risk as "miniscule."[57] Moreover, instead of a federally coordinated effort, the response was largely left to individual states:

> "'Every governor is out there on his or her own working to build the same programs that are being built next door,' said Reed Schuler, a senior advisor to Democratic Washington Gov. Jay Inslee. 'The federal government's efforts range from a little bit of backup to not even being present.'"[58] Similarly, Republican Maryland Gov. Larry Hogan has written, "as the White House failed to…draw up a 50-state strategy…every governor went their own way, which is how the United States ended up with such a patchwork response."[59]

Another emergency management expert stated, "Let's be clear: The federal government has failed. If we maintain the status quo, the cavalry is not coming. Pandemic prevention efforts were ineffective. Pandemic preparedness efforts were ineffective. Pandemic coordination efforts were ineffective."[60]

The absence of a national plan, exacerbated by the failure of key institutions, has added to the devastating harm caused by the coronavirus.

3) Failure of Key Institutions

Well beyond HHS's initial missteps, two key elements under the aegis of HHS—the Centers for Disease Control and Prevention and the Strategic National Stockpile—that are central to dealing with a pandemic performed inadequately.

As described in multiple media: "The CDC, long considered the world's premier health agency, made early testing mistakes that contributed to a cascade of problems that persist today as the country tries to reopen. It failed to provide timely counts of infections and deaths, hindered by aging technology and a fractured public health reporting system. And it hesitated in absorbing the lessons of other countries, including the perils of silent carriers spreading the infection."[61]

The coronavirus would have been a very difficult test for even the most ready and agile agency, but the CDC appears to have suffered from a culture that was not aligned for quick response:

> "[A]ccording to current and former employees and others who worked closely with the agency, the CDC is risk-averse, perfectionist, and ill-suited to improvising in a quickly evolving crisis—particularly one that shuts down the country and paralyzes the economy…'It's not our culture to intervene,' said Dr. George Schmid, who worked at the agency off and on for nearly four decades. He

55 Daniel M. Gerstein, *The Strategic National Stockpile and COVID-19 Rethinking the Stockpile*, RAND, June 23, 2020, 7, https://www.rand.org/content/dam/rand/pubs/testimonies/CTA500/CTA530-1/RAND_CTA530-1.pdf.

56 "Secretary Azar Declares Public Health Emergency for United States for 2019 Novel Coronavirus," Department of Health and Human Services, January 31, 2020, https://www.hhs.gov/about/news/2020/01/31/secretary-azar-declares-public-health-emergency-us-2019-novel-coronavirus.html.

57 Jayne O'Donnell, "Top Disease Official: Risk of Coronavirus in USA is 'Minuscule,'" *USA Today*, February 17, 2020, https://www.usatoday.com/story/news/health/2020/02/17/nih-disease-official-anthony-fauci-risk-of-coronavirus-in-u-s-is-minuscule-skip-mask-and-wash-hands/4787209002/.

58 Quoted in Dan Goldberg And Alice Miranda Ollstein, "A Dangerous New Chapter of the Outbreak: Every State for Itself," *Politico*, July 14, 2020, https://www.politico.com/news/2020/07/14/states-look-to-trump-for-a-national-plan-to-fight-coronavirus-361906.

59 Governor Larry Hogan, "Fighting Alone," *Washington Post*, July 16, 2020, https://www.washingtonpost.com/outlook/2020/07/16/larry-hogan-trump-coronavirus/?arc404=true.

60 Thomas Henkey, "Perspective: It Is Not Too Late to Get the Coronavirus Response Right," Homeland Security Today, April 1, 2020, https://www.hstoday.us/subject-matter-areas/emergency-preparedness/perspective-it-is-nottoo-late-to-get-the-coronavirus-response-right/.

61 Eric Lipton, et al, "The CDC Waited Its Entire Existence for This Moment. What Went Wrong?" *New York Times*, June 3, 2020, https://www.nytimes.com/2020/06/03/us/cdc-coronavirus.html.

> described it as increasingly bureaucratic, weighed down by 'indescribable, burdensome hierarchy.'"[62]

Adding to the lack of agility, the CDC has serious technology deficiencies. One of the keys to dealing with a pandemic like COVID-19 is getting the right data promptly. "But that has proved difficult for the [CDC's] antiquated data systems, many of which rely on information assembled by or shared with local health officials through phone calls, faxes, and thousands of spreadsheets attached to emails. The data is not integrated, comprehensive, or robust enough, with some exceptions, to depend on in real time."[63]

In significant part, this lack of capacity to collect and analyze data arose from a deficiency of resources: "For years, federal and state governments have not invested enough money to ensure that the nation's public health system would have critical data needed to respond in a pandemic. Since 2010, for example, grants to help hospitals and states to prepare for emergencies have declined."[64] Again, this failure was not because the problem was unknown. "In 2019, more than 100 public health groups pressed congressional leaders to allocate $1 billion over a decade to upgrade the infrastructure."[65]

Moreover, lack of resources does not entirely explain the CDC's data failures. Other entities demonstrated the capability to quickly collect and analyze relevant data. For example, "many officials turned to Johns Hopkins University, which became the primary source for up-to-date counts. Even the White House cited its numbers instead of the CDC's lagging tallies."[66]

Similarly, the Strategic National Stockpile, under the authority of the HHS assistant secretary for preparedness and response, was not prepared for a pandemic. As one account described:

> "At the beginning of the coronavirus outbreak, the stockpile contained only about 12 million of the 3.5 billion N95 masks that federal officials estimated the healthcare system would need to fight this pandemic back in March… But the stockpile was never intended to be the nation's great savior. It wasn't supposed to provide all of the nation's medical supply needs for a multi-month pandemic. Congress never doled out enough money for it to do so. Instead, the officials who monitored the national stockpile were hopeful that hospitals were making their own stockpiles. But to save money, they largely weren't. In that context, the skimpy mask supply in the Strategic National Stockpile is not the thing that derailed the American response to COVID-19. Rather, it's one of a series of planning failures that created the crisis we're in today."[67]

Another analysis stated, "Although the stockpile has a stated purpose that includes providing support during a pandemic response, the stockage levels and types of vaccines and therapeutics indicate a predisposition toward response to a bioterrorism event or a much smaller outbreak event, such as the 2014 Ebola response."[68]

That the stockpile failure could have been avoided is demonstrated by how the federal government has since responded to materiel shortages, particularly by using authorities available to the Defense Department under the Defense Production Act. In testimony, "Based on the investments made by the department, [DOD officials] told the House panel, an increase in production of 450 million masks a year will be attained by October, with a rate of more than 800 million masks per year by January. 'Starting in 2021, we anticipate our total domestic production to be in excess of a billion per year,' [officials] said."[69]

The deficiencies at the CDC and with respect to the stockpile were exacerbated by political leaders who were slow to accept the need for significant steps to contain the virus. Not only was the Administration slow to recognize the dangers—the President stated on March 10, "It will go away. Just stay calm. It will go away,"[70] but many state and local leaders—governors and mayors—were slow to generate shelter in place and similar orders. By way of example, in New York City, the mayor in early March was "encouraging New Yorkers to…get out on the town despite

62 Ibid.

63 Ibid.

64 Ibid.

65 Ibid.

66 Ibid.

67 Olga Khazan, "Why We're Running Out of Masks," *The Atlantic*,April 10, 2020, https://www.theatlantic.com/health/archive/2020/04/why-were-running-out-of-masks-in-the-coronavirus-crisis/609757/.

68 Gerstein, *The Strategic National Stockpile*, 11.

69 C. Todd Lopez, "Domestic N95 Mask Production Expected to Exceed 1 Billion in 2021," DOD News, June 10, 2020, https://www.defense.gov/Explore/News/Article/Article/2215532/domestic-n95-mask-production-expected-to-exceed-1-billion-in-2021/.

70 Remarks by President Trump After Meeting with Republican Senators, The White House, March 10, 2020, https://www.whitehouse.gov/briefings-statements/remarks-president-trump-meeting-republican-senators-2/.

Coronavirus."[71] One analysis has concluded that if shelter-in-place steps had been taken even one week earlier than mid-March, some thirty-six thousand deaths could have been avoided.[72]

4. Biodefense Challenges

Like cyber, the threat of a biological attack has been a long-standing concern to the national security community, but it has never obtained the attention given to nuclear, conventional, counter-terror, or counterinsurgency issues. There was heightened attention arising from the anthrax incidents shortly after the September 11 attacks, but for the most part there has been limited focus on potential biological attack. This lack of emphasis persists despite severe warnings from high level actors such as Richard Danzig, former US secretary of the Navy, who wrote:

> "[B]iological weaponry [is] on the same plane as nuclear weapons; they can be catastrophic, whether measured by deaths and injuries or economic, operational, or psychological effects…An aerosol attack using a kilogram of anthrax…configured to disperse fairly efficiently, or an attack that introduced smallpox…into our presently unvaccinated population could reasonably be expected to kill tens of thousands of people. It could take decades after an anthrax attack before [the targeted area] could be restored to the point where deaths were not caused by residual contamination."[73]

In short, the biological threat is significant, and the concerns it raises come from both nations and non-state actors.[74] As the Bipartisan Commission on Biodefense highlighted:

> "China, Iran, North Korea, Russia, and Syria continue to engage in dual-use or biological weapons-specific activities and are failing to comply with the [Biological Weapons Convention] BWC…[T]errorist organizations, domestic militia groups, and lone wolves have expressed intent to use and shown some capacity to develop biological weapons. Advances in science have led to a convergence of biology and chemistry, and an ability (through synthetic biology) to create and combine agents. All of this has expanded the number and types of potential biological weapons and made it more difficult to fully comprehend the enormity of the threat."[75]

The biological threat is significant, and the concerns … come from both nations and non-state actors."

E. Future Risks

The future risks facing the United States are substantial. As many have pointed out, a number of conditions make future pandemics increasingly likely. In a recent report, Gavi, the Vaccine Alliance, stated that "despite huge scientific and medical advances, today the potential for diseases to spread is actually increasing, and therefore so too is the risk of outbreaks escalating into epidemics or pandemics. A massive increase in globalization and connectivity has meant that a virus can spread from one side of the world to another in mere hours."[76] Key factors identified by Gavi are global travel, urbanization, climate change, increased human-animal contact, and health worker shortages.[77]

As disruptive as the coronavirus has been, future risks could be even greater. Michael Osterholm has stated, "some future microbial outbreak will be bigger and deadlier still. In other words, this [current COVID-19] pandemic is probably not the 'Big One,' the prospect of which haunts the nightmares of epidemiologists and public health officials everywhere."[78] The Global Preparedness Monitoring Board likewise has warned, "The world is at acute risk for devastating regional or global disease epidemics or

71 Bill de Blasio (@BilldeBlasio), "Since I'm encouraging New Yorkers to go on with your lives + get out on the town despite Coronavirus, I thought I would offer some suggestions. Here's the first…," Twitter, March 2, 2020, https://twitter.com/BilldeBlasio/status/1234648718714036229.

72 James Glanz and Campbell Robertson, "Lockdown Delays Cost at Least 36,000 Lives, Data Show," *New York Times*, May 20, 2020, https://www.nytimes.com/2020/05/20/us/coronavirus-distancing-deaths.html.

73 Richard J. Danzig, *A Policymaker's Guide to Bioterrorism and What to Do About It*, National Defense University, December 2009, 4-5, https://ndupress.ndu.edu/Portals/68/Documents/occasional/CTNSP/A-Policymakers-Guide.pdf?ver=2017-06-16-143201-930.

74 *National Biodefense Strategy*, 2018, 3, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf ("nation-states and terrorist groups have found value in pursuing biological weapons, and there can be no confidence that will change in the future").

75 Bipartisan Report of the Blue Ribbon Study Panel On Biodefense, *A National Blueprint for Biodefense*, October 2015, 4, https://biodefensecommission.org/wp-content/uploads/2015/10/NationalBluePrintNov2018-03.pdf.

76 "5 Reasons Why Pandemics Like COVID-19 are Becoming More Likely," Gavi, the Vaccine Alliance, June 2020, https://www.gavi.org/vaccineswork/5-reasons-why-pandemics-like-covid-19-are-becoming-more-likely.

77 Ibid.

78 Osterholm and Olshaker, "Chronicle of a Pandemic Foretold."

pandemics that not only cause loss of life but upend economies and create social chaos."[79] An adversarial-generated biological attack could be equally devasting.

Moreover, the danger is not limited to a future virus or biological attack. As the United States grows ever more reliant on information technology, a major cyberattack could likewise generate extraordinarily disruptive consequences for the country. As the Cyberspace Solarium Commission has underscored, "[A] significant cyberattack can be global in nature, requiring that nations simultaneously look inward to manage a crisis and work across borders to contain its spread."[80]

Finally, there are the long-term risks posed by China's disruptive state-driven model, including its pervasive presence in the supply chain, use of cyber espionage, and impact of unfair practices on market competition. Without appropriate response, each of these—alone or in combination—could undercut the economic strength and national security of the United States.

The discussion below proposes a strategic and operational framework for effective resilience focused on key critical infrastructures that would mitigate the consequences of such disruptions and dangers.

79 Global Preparedness Monitoring Board, *A World At Risk*, September 2019, 11, https://apps.who.int/gpmb/assets/annual_report/GPMB_annualreport_2019.pdf.

80 Cyberspace Solarium Commission, *Cybersecurity Lessons From The Pandemic*, May 2020, i, https://drive.google.com/file/d/1wCHVtlFlw84uZIPOTZe2nkdGau15fLAQ/view.

IV. EFFECTIVE RESILIENCE AND NATIONAL STRATEGY

Effective resilience means the capacity to prepare for and withstand shocks of the magnitude of a major pandemic or equivalent, such as a major cyberattack, with any resulting disruption significantly less than that caused by COVID-19.[81] Effective resilience also needs to encompass longer-term challenges, including those posed to the economy, particularly those from Chinese cyber espionage and state-driven economic practices. To achieve those goals, effective resilience needs to be a major element of national strategy. Its accomplishment will require focused objectives, operational effectiveness, and appropriate resourcing. Consequentially, changes will need to be undertaken at the federal, state, and local levels, as well as in the private sector. Health sector resilience is a high priority. In addition, achieving resilience in the economic and security sectors will require evaluation of key critical infrastructure supply chains, cyber and biological security, and the impact of China on the US economy and security.

To accomplish the end of effective resilience, the way forward should include:

1) a Strategic Framework for Key Critical Infrastructure Resilience;

2) a Strategic Framework for Health Sector and Biological Resilience; and

3) establishment by Congress of a Resilience Commission.

The elements of each of these are set forth in detail in the discussions below.

A. A Strategic Framework for Key Critical Infrastructure Resilience

One important lesson of the pandemic is that it is important to enhance the resilience of nationally critical sectors. The key critical infrastructures of defense, energy (electric grid and pipelines), food, finance, health, information and communications technology, transportation, and water ("key critical infrastructures") are of highest importance to the economy and warrant priority review to assure resilience against both shocks and over the longer term. To create an appropriate response to future pandemics or comparable national disruptions including longer-term resilience issues requires establishing: 1) Resilient Industrial Bases for the key critical infrastructures including a plan for the resilience of nationally critical supply chains; 2) establishing resilience stress tests for companies in key critical infrastructures; and 3) development and implementation of cybersecurity resilient architectures for key critical infrastructures. A pervasive question throughout each of these issues is the appropriate strategy for dealing with China.

> "Effective resilience means the capacity to prepare for and withstand shocks of a magnitude of a pandemic … [and] longer-term challenges … to the economy."

1) Resilient Industrial Bases for Key Critical Infrastructures

The federal government has designated sector-specific agencies for each of the key critical infrastructure sectors.[82] Each sector-specific agency should undertake—under a Congressional mandate if necessary—a review of the key critical infrastructure sector under its auspices that will lead to the Congressionally approved establishment of an appropriate Resilient Industrial Base for each sector. A Resilient Industrial Base is a sector capability, including tailored governmental support, to maintain resilience in the face of adversarial shocks and over the long-term. Sectors vary significantly, so there would be no single model. The nature of governmental support could range from contractual arrangements to the making of loans or investments to tax credits. It could also entail the use of authorities such

81 One comprehensive review of the literature on resilience described several useful wordings including: "resilience is the capacity of a system to anticipate, adapt, and reorganize itself under conditions of adversity in ways that promote and sustain its successful functioning." Michael Ungar, "Systemic Resilience: Principles and Processes for a Science of Change in Contexts of Adversity, *Ecology and Society*, 2018, https://www.ecologyandsociety.org/vol23/iss4/art34.

82 US Department of Homeland Security: Cybersecurity and Infrastructure Security Agency, "Sector-Specific Agencies," 2018, https://www.cisa.gov/sector-specific-agencies.

as the Defense Production Act when circumstances warrant, or the imposition of tariffs and other methods to limit unfair competition such as China may present. To reiterate, no Resilient Industrial Base for any sector should be established without appropriate Congressional action.

In undertaking the development of Resilient Industrial Base strategies, each sector-specific agency should evaluate three sets of issues for its sector. First would be a determination of the manufacturing, services, and other capacities required throughout the supply chain to assure availability and integrity of products and services—and the types of incentives and support necessary to achieve those capacities. Second would be a process for creation of future capabilities. This would focus on supporting research and development so that resilience will be maintained in the face of emerging and advanced technologies—including the role of government in generating the required research and development. Third would be the need to evaluate which entities to exclude from, or limit their participation in, the supply chain for the sector—an issue most obviously concerned with China.

As a consequence of the reviews, the relevant sector-specific agency would undertake to work with Congress to establish a sectoral Resilient Industrial Base in order to assure the ability of the sector to operate effectively both in the face of shocks and over the longer term. In this regard, the Defense Industrial Base provides something of a guide, as maintaining its resilience is a focus for every administration and Congress. While not enacted as of this writing, the Senate version of the FY2021 National Defense Authorization Act has several provisions directed to that sector. Those provisions, which will perhaps help to create a model for other sectors, include requiring assessment of various methods such as subsidies, investments, and provision of credit to enhance the defense industrial base (defined to include "friendly and capable allies and partners"); requiring a strategy for microelectronics manufacturing in the United States; and assessing economic and legal "structures shaping the capacity of the national security innovation base."[83] The Cyberspace Solarium Commission similarly came to the conclusion that an industrial base strategy was needed for the information and communications technology sector:

> "Congress should direct the U.S. government to assess the United States' information and communications technology (ICT) supply chain and develop and implement an ICT industrial base strategy to reduce dependency and ensure greater security and availability of these critical technologies. This strategy should focus on ensuring the availability and integrity of trusted components, products, and materials necessary for the manufacture and development of ICTs deemed most critical to national and economic security."[84]

Other sectors need a conceptually similar strategic approach, though given the differences among sectors, the particulars likely will be quite diverse. In analyzing the requirements of a sector-specific Resilient Industrial Base, a sensible starting point is to recognize that, under normal circumstances, free market mechanisms resolve this question. However, the issues that have arisen in the context of the pandemic with respect to health (lack of needed materials), food (the need to put certain parts of the food chain under government control through the Defense Production Act[85]), and transportation (container shipping being impeded[86]) are indications that normal circumstances do not always apply. These differentiated circumstances arise as a result of a shock or because of longer-term market challenges. The sector-specific agency will need to determine what will be required to assure resilience when those "normal circumstances" are no longer applicable.

A sector-specific agency undertaking a sectoral supply chain review will need to evaluate the risks presented throughout the supply chain, and the costs and benefits of offsetting such risks. Such an analysis needs to be forward looking, accounting for the risks and benefits that might arise from the development of advanced and emerging technologies, so as to assure dynamic resilience over the longer term.

The pandemic itself generated three types of supply chain issues: a sudden increase in demand, as exemplified by the increased demand for medical supplies; a breakdown in supply when the lockdowns limited worker availability and when the virus affected transportation across global routes; and an impact on supply caused by unreliable or untrustworthy suppliers, an issue which can arise under multiple circumstances but one which China presented. Each of those are important areas for review. However, the resilience issues are broader and the DOD/interagency

83 National Defense Authorization Act FY 2021, Sections 801 et seq. including sections 801, 802, 807, https://www.armed-services.senate.gov/imo/media/doc/S4049%20-%20FY%202021%20NDAA.pdf.

84 *Cyberspace Solarium Commission*, March 2020, 88, https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtlY/view.

85 The White House, "Executive Order on Delegating Authority Under the DPA with Respect to Food Supply Chain Resources During the National Emergency Caused by the Outbreak of COVID-19," April 28, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-delegating-authority-dpa-respect-food-supply-chain-resources-national-emergency-caused-outbreak-covid-19/.

86 Mike Wackett, "'No hope' of bounce-back in demand for container shipping this year," *The Lodestar*, May 26, 2020, https://theloadstar.com/no-bounce-back-in-demand-for-container-shipping-this-year/.

supply chain review, noted above, had a more comprehensive, though overlapping, analysis, identifying ten types of supply chain risks. Those include risks arising from sole and single source suppliers; fragile suppliers (financially challenged); fragile markets (cannot meet foreign competition); capacity constrained markets; foreign dependency; diminishing sources/suppliers of material necessary to components or final products; gaps in human capital; lack of sufficient specialized capital equipment; and insecurity of product, whether physical or cyber.[87]

As the DOD/interagency supply chain review implies, in analyzing supply chain resilience for critical infrastructures a sector-specific agency should look at the entirety of the types of challenges to supply chain resilience in their particular sector. However, the objective of such a review is not to resolve all the problems of the sector, but rather to assure its resilience. Accordingly, the sector-specific agency should focus its review on those portions of the supply chain—including both hardware materials and software—most relevant to the resilient output of the sector.

a. Resilient Industrial Bases and the Supply Chain

There are some obvious starting points to a supply chain review. First, it is useful to recognize that supply chains exist for reasons that presumably make sense to the firms involved. Change will not be without costs and may have to be accomplished over time. The business reasons for creating the chain need to be understood. That does not mean that there should not be change, but it does mean that the costs of change warrant review. Second, at the firm level, "having several suppliers in multiple locations is a strategy for robustness…[and] having compatible standards boosts resilience by having a stock of standardized inputs that are easier to replace."[88] Third, and hardly a surprise when evaluating global supply chains, "having a diversified source of imports from alternative supplying countries would increase the resilience of supply for…firms. Otherwise, if there is a major disruption affecting this sole supplying country…importers would have no plan B."[89]

In addition to utilizing the concept of diversification as the foregoing suggests, the sector-specific agency should evaluate how confronting the different types of potential disruption will call for different answers. For example, in dealing with the issue of potential sudden demand increase, policymakers will want to utilize a combination of stockpiling and surge capability. When focused on potential transportation constraints, there may be routes that nonetheless can be expected to be reliable, and other circumstances where product needs to be sourced close to demand. Each of these sets of considerations raises the question of which supply chains—or portions of the supply chain—need to be in the United States, which can rely on allies and close partners, and which can be market-driven. As a general proposition, globalization has meant that supply chains include multiple countries, and reliance on allies is regularly undertaken in multiple areas, including in the defense sector where maintaining the Defense Industrial Base is quite important.[90] Accordingly, even in the context of establishing a Resilient Industrial Base for a particular sector, it should be generally satisfactory to include allies (and reliable partners) in the supply chain—though the precise contours of what and how much should be maintained in the United States will require a granular review by the sector-specific agency.[91]

b. Resilient Industrial Bases and China

The most important longer-term resilience issues arise from the challenges presented by China. In evaluating how to respond in the context of Resilient Industrial Bases, it will be useful, and necessary, to consider actions that the federal government has already taken and whether they present a model for future approaches. At the sectoral level, the current administration has issued two significant executive orders: one directed to the information and communications technology sector and the other to the bulk-power system. In brief substance, the orders establish a framework to prohibit transactions in each of these arenas with a foreign adversary that poses significant risk. More specifically, they require the relevant cabinet secretary to

87 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, 46, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

88 Lucian Cernat Oscar Guinea, "On Ants, Dinosaurs, and How to Survive a Trade Apocalypse," European Centre for International Political Economy, July 2020, https://ecipe.org/blog/how-survive-trade-apocalypse/.

89 Guinea, "On Ants, Dinosaurs, and How to Survive a Trade Apocalypse."

90 For example, the United States has a National Technology and Industrial Base with the Australia, Canada, and the United Kingdom. Congressional Research Service, *Defense Primer: The National Technology and Industrial Base*, January 31, 2020, https://crsreports.congress.gov/product/pdf/IF/IF11311. Even high technology programs can be supplied by allies. For example, there is a global supply chain for the advanced F-35 fighter aircraft; "Suppliers in all nine of the program's partner countries are producing F-35 components for all aircraft, not just those for their country." Lockheed Martin, "The Centerpiece of 21st Century Global Security" 2020, https://www.f35.com/global.

91 The Cyberspace Solarium Commission found that "the shortages of critical resources during the COVID-19 pandemic have validated the commission's finding that the United States must do more to ensure that the necessary resources are available before a crisis. Developing and implementing an information and communications technology industrial base strategy to identify critical dependencies and to direct strategic investments will ensure the industrial capacity needed to alleviate those critical dependencies." "Executive Summary," Cyberspace Solarium Commission, March 2020, 7, https://drive.google.com/file/d/1c1UQI74Js6vkfjUowI598NjwaHD1YtIY/view.

bar any transaction with a foreign adversary regarding the bulk-power system or information and communications technology or services that:

> "poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance [of the bulk-power system or information and communications technology or services];"
>
> "poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the economy of the United States;" or
>
> "otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."[92]

"In evaluating … key critical infrastructure supply chains … there are certain sectors from which China should be … excluded and others where a 'China plus one' strategy could be satisfactory."

As of this writing, the regulations implementing the executive orders are not final in the case of the information and communications technology order,[93] and not yet issued in the case of the bulk-power system. Accordingly, the precise mechanisms for implementation are not yet clear.

No similar sectoral executive orders exist for the key critical infrastructures of food, finance, health, pipeline, transportation, and water, though each sector will be constrained by the limits on ICT transactions, and though the defense sector already operates with multiple "Buy America" requirements.[94] However, the risk to the nation as a whole varies depending on the sector in question. Accordingly, a differentiated approach should be utilized in evaluating appropriate responses to Chinese presence in different key critical infrastructure supply chains. As discussed below, there are certain sectors from which China should be entirely excluded and others where less stringent requirements such as a "China plus one" strategy could be a satisfactory approach.

To begin, for strategic sectors vital to national security or other critical national objectives, Chinese products, components, and services should be excluded from the supply chain unless the use is approved by the US government. That limitation would encompass the defense sector and the intelligence community.[95] The sector-specific agencies would need to determine whether other key critical infrastructure supply chains should be included in the strategic category.

Secondly, even if a sector might not be designated strategic for national security reasons, the question of China's exclusion from the supply chains for key critical infrastructures should nonetheless be evaluated at a more granular level. This is particularly true in the context of software supply chains. Software frequently includes flaws creating vulnerabilities for exploitations, and supply chains are a mechanism for inserting maliciously intended flaws.[96] Congress should require that the sector-specific agencies prohibit the use of Chinese software in elements of the supply chain that could lead to exploitations posing significant risks.

Hardware and other materials from China also need to be reviewed, especially in situations where China is the sole or dominant source. As noted above, Congress has recently required under section 3112 of the CARES Act that

92 The White House, "Executive Order on Securing the United States Bulk-Power System," May 20, 2020, section 1(a)(ii), https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/; The White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, section 1(a)(ii), https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

93 US Department of Commerce, *Proposed Rule, Securing the Information and Communications Technology and Services Supply Chain*, November 27, 2019, https://www.federalregister.gov/documents/2019/11/27/2019-25554/securing-the-information-and-communications-technology-and-services-supply-chain.

94 The White House, "Executive Order on Maximizing Use of American-Made Goods, Products, and Materials," July 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maximizing-use-american-made-goods-products-materials/. One analysis of the impact of the order is found at David Gallacher, "Buy American" (Again): New Executive Order Requires Changes (By 2020)," July 31, 2019, https://www.governmentcontractslawblog.com/2019/07/articles/baa-and-taa/baa-buy-american-again/

95 There have been a number of determinations by the federal government limiting the use of products from China including, for example, a rule prohibiting federal agencies from contracting with companies that use in their systems telecommunications equipment produced by Huawei Technologies Company, ZTE Corporation, or their affiliates. Federal Acquisition Regulatory Council, *Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment*, July 14, 2020, https://www.federalregister.gov/documents/2020/07/14/2020-15293/federal-acquisition-regulation-prohibition-on-contracting-with-entities-using-certain.

96 See Herr, Lee, Loomis, and Scott, *BREAKING TRUST*, 6.

certain pharmaceutical providers have a resilience plan.[97] A resilience plan mandate could be expanded to other key critical infrastructures, with the further requirement that designated firms would have to avoid a situation in their supply chains where there is sole or dominant reliance on China.[98] Precisely how to define "dominant" would require further analysis, but the basic idea is that a shutdown of supply by China should not cause a sweeping impact on the relevant sector.

One way to accomplish this would be to require dual sourcing by adding a mandate for the supply chain to include a "plus one" country. Companies would, therefore, not be forced to entirely upend their supply chains that rely on China but could be required to expand them to include other countries. Doing so would incur costs but has concomitant assurance benefits for firms, as well as making sectors more resilient as a whole. The amount of any required expansion to "plus one" countries could be increased over time giving supply chains the capacity to adjust smoothly. Accordingly, for the key critical infrastructures, Congress should require dual sourcing with the supply chain including a "plus one" country so that China is not in a sole or dominant position.

c. Resilient Industrial Bases—Innovation and Long-term Resilience

A useful illustration of the potential relationship between innovation and resilience comes from the testimony of Dr. Janet Woodcock of the Federal Drug Administration (FDA) who described the benefits that could accrue to supply chain resilience from investment in one type of advanced technology:

> "Advanced manufacturing is the use of innovative technology to improve products and processes… Advanced manufacturing offers many advantages over traditional pharmaceutical manufacturing, and if the United States invests in this technology, it can be used to reduce the Nation's dependence on foreign sources of [active pharmaceutical ingredients] API's, increase the resilience of our domestic manufacturing base, and reduce quality issues that trigger drug shortages or recalls…By supporting the growth of advanced manufacturing in the United States, we can reduce our dependence on China and other overseas manufacturers for APIs as well as improve the resilience and responsiveness of our manufacturing base and reduce drug shortages."[99]

"Advanced manufacturing offers many advantages … and if the United States invests in this technology, it can be used to reduce … dependence on foreign sources."

As Dr. Woodcock's testimony indicates, enhancing innovation will enhance the capacity of key critical infrastructures to deal with shocks and also to remain competitive over the long term. Another example would be the increased use of additive manufacturing (3D printing) in supply chains.

Multiple studies have recommended ways to enhance innovative efforts by both public and private entities,[100] and while the particulars may differ among sectors, there are a number of actions that can be taken by the Congress, the administration, and the sector-specific agency. These include increased funding for basic research and development; increasing access to international research and development; and expanding government projects into

97 Coronavirus Aid, Relief, and Economic Security Act, Section 3112, "Additional Manufacturer Reporting Requirements In Response To Drug Shortages," https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

98 One proposal focused on standards for the Internet of Things provided the contours of an approach: "This paper proposes to apply regulatory pressure to domestic technology distributors to drive adoption of security standards throughout their supply chains. This *reverse cascade* enforces standards back to foreign manufacturers by preventing domestic sale or distribution of products that don't adhere to the standard. The reverse cascade's effectiveness is amplified where these supply chains are unusually concentrated in a single or small handful of firms. This approach addresses US regulators' limited influence in foreign jurisdictions and relinquishes the need to monitor hundreds, if not thousands, of overseas manufacturers directly." Nathaniel Kim, Trey Herr, and Bruce Schneier, *The Reverse Cascade: Enforcing Security On The Global Iot Supply Chain*, *Atlantic Council*, June 2020, 1-2, https://www.atlanticcouncil.org/in-depth-research-reports/report/the-reverse-cascade-enforcing-security-on-the-global-iot-supply-chain/.

99 *Safeguarding Pharmaceutical Supply Chains in a Global Economy*, US House Committee on Energy and Commerce, Subcommittee on Health, 116th Cong. (2019) (statement of Janet Woodcock, M.D., Director - Center for Drug Evaluation and Research, Food and Drug Administration), 8-9, https://www.fda.gov/news-events/congressional-testimony/safeguarding-pharmaceutical-supply-chains-global-economy-10302019.

100 See, e.g., James Manyika and William H. McRaven, "Innovation and National Security: Keeping Our Edge," Council on Foreign Relations, 2019, https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf, and Kramer and Wrightson, Jr., *Innovation, Leadership and National Security*.

key new areas.[101] Moreover, corporations can be incentivized through tax credits for research and development efforts or through innovative finance such as the issuance of tax-free "technology bonds," thereby lowering the cost of borrowing.[102] Public-private efforts could be expanded by establishing manufacturing test beds and prototyping centers focused on developing innovative capabilities.[103] The sector-specific agencies should evaluate these and other approaches, and create a proposed agenda for Congressional action that could be used to support the key critical infrastructures.

China presents an additional challenge for long-term resilience that can affect key critical infrastructures, but can have wider consequences. It will be critical over the long term to ensure that United States firms can compete effectively in the market and are not undercut by Chinese firms relying on unfair advantages brought about by China's state-directed economy. As noted above, China extensively utilizes subsidies, intellectual property theft, and restrictions in its home market to create such unfair market advantages, and those efforts give Chinese firms the ability to significantly underprice market-driven firms. The United States does not want to be in a position where its key critical infrastructures have to rely on China, especially for advanced and emerging technologies. In order to assure long-term resilience of US firms in those competitive markets which are unfairly affected by such Chinese state-directed economic practices—most importantly, the markets for advanced and emerging technologies such as artificial intelligence, adaptive manufacturing, genomics, robotics, and quantum computing—frameworks need to be established that will have selective, but effective, offsetting impact on the improper advantages of Chinese firms. These frameworks would include the use of import restraints and/or selective focused tariffs, so as to ensure a level playing field for US firms.[104] There have been a number of actions already by the federal government that limit the engagement of Chinese firms in US markets, including through the use of tariffs as well as restrictions on particular firms. While the President's authorities are very broad, Congress should enact legislation that will make it the policy of the United States to respond to such predatory practices and to require the sector-specific agencies to determine what offsetting actions, including import restraints and/or tariffs, need to be undertaken to assure the resilience of the key critical infrastructures and their supply chains.

In sum, as Dr. Woodcock's testimony indicates, the benefits from the types of actions recommended above could be significant both for innovation generally and, more specifically, for supply chain resilience for key critical infrastructures.

> "Resilience stress testing should be established for the key sectors of defense, energy, food, health, information and communications technology, transportation and water."

2. Resilience Stress Tests for Key Critical Infrastructures

Resilience stress tests have been utilized in the financial sector since the financial crisis of 2008-2009.[105] A conceptually similar approach for resilience stress testing should be established for the key sectors of defense, energy, food, health, information and communications technology, transportation and water. As one analysis stated:

> "The global pandemic has exposed serious flaws in supply chains, including critical ones for industries such as pharma[ceuticals] and medical supplies. Shortages of personal protective equipment for health workers and ventilators in hospitals are the most prominent ones. To prevent this problem from occurring again when the next disaster strikes, governments should consider establishing a stress test for companies that provide critical goods and services that's akin to the stress tests for banks that the U.S. government and European

101 An important report by one commissioner and staff members of the National Security Commission on Artificial Intelligence has a series of recommendations as to potential uses of artificial intelligence for pandemic response and preparedness including enabling "AI-powered advanced manufacturing." Jason Matheny, Olivia Zetter, Tess deBlanc-Knowles, and Michael Garris, *The Role of AI Technology in Pandemic Response and Preparedness: Recommended Investments and Initiatives*, National Security Commission on Artificial Intelligence, 13, https://drive.google.com/file/d/153DUHToD4zoM_GXe9MWGNKzend7Tsl2o/view.

102 A technology bond would have the proviso that the funding is used for a designated technological purpose and, if that is done, the interest would be tax free to investors.

103 Test beds established by the government or through a public-private effort could dramatically shorten the timeline and expense for innovation as they can provide a place for entrepreneurs and companies to test and refine manufacturing process ideas without having to build their own facility at a high (and sometimes prohibitive) cost. Kramer and Wrightson, Jr., *Innovation, Leadership and National Security*, 20.

104 Kramer, *Managed Competition*, 29.

105 Board of Governors of the Federal Reserve System, *Financial Stability Report*, May 2020, https://www.federalreserve.gov/publications/files/financial-stability-report-20200515.pdf.

> Union instituted after the 2008 financial crisis. This test should focus on the resilience of companies' supply chains."[106]

As noted, Congress has taken a first step with the passage of section 3112 of the CARES Act which requires "a redundancy risk management plan that identifies and evaluates risks to the supply of the drug."[107] However, while having a plan is worthwhile, having a plan that will work in the face of significant stress is the real goal. To ensure that, having appropriate standards which are reviewed periodically by an independent entity, as is done for financial stress testing, is critical.

The standards for such a resilience stress test approach would have to be determined and would likely differ among the different key critical infrastructures. Among other considerations would be: how much of an industry sector should be included, for example, only firms of a certain size or those with certain characteristics, such as sole source producers; how deep into the supply chain should resilience testing go; how much output would need to be sustained; over what period should disruption be expected; and how much should be accomplished in the United States versus how much reliance could be placed on allies and close partners. The standards could also be used to enforce the exclusions and limits on China in the supply chain as discussed in prior sections of this report. Additionally, the standards could include affirmative requirements. One possibility would be to require covered firms to have pandemic insurance—essentially business interruption insurance only payable in the event of a pandemic—that could be used, for example, to limit the impact on employment.[108]

Congress should require the sector-specific agencies to develop resilience stress tests for their sector. Doing so is a non-trivial task that requires understanding the full supply chain. A resilience supply chain stress test will need to consider raw materials sources, midstream components, and finished products.[109] In undertaking the necessary mapping:

> "The goal should be to go down as many tiers as possible, because there may be hidden critical suppliers the buying firm is not aware of. The map should also include information about which activities a primary site performs, the alternate sites the supplier has that could perform the same activity, and how long it would take the supplier to begin shipping from the alternate site."[110]

Each segment in the chain needs to be reviewed because "[w]hen any link in the chain breaks, upstream and downstream suppliers and consumers are impacted too."[111]

Mapping will, therefore, undoubtedly require significant resources:

> "The required resources for supply network mapping are expensive. Many companies and leaders talk about the need to do supply network mapping as a risk-mitigation strategy, but they have not done so because of the perceived large amount of labor and time required. Executives of a Japanese semiconductor manufacturer told us that it took a team of 100 people more than a year to map the company's supply networks deep into the sub-tiers following the earthquake and tsunami in 2011."[112]

106 Simchi-Levi and Simchi-Levi, "We Need a Stress Test."

107 The statute reads: "Each manufacturer of a drug [that is critical to the public health during a public health emergency] or of any active pharmaceutical ingredient or any associated medical device used for preparation or administration included in the drug, shall develop, maintain, and implement, as appropriate, a redundancy risk management plan that identifies and evaluates risks to the supply of the drug, as applicable, for each establishment in which such drug or active pharmaceutical ingredient of such drug is manufactured." Coronavirus Aid, Relief, and Economic Security Act, Section 3112, "Additional Manufacturer Reporting Requirements In Response To Drug Shortages," https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

108 Evan Ratliff, "We Can Protect the Economy From Pandemics. Why Didn't We?" *Wired*, June 16, 2020, https://www.wired.com/story/nathan-wolfe-global-economic-fallout-pandemic-insurance/.

109 One useful mapping analysis reviewed the supply chain of lithium batteries, dividing it into "raw materials" such as cobalt, nickel, manganese, and graphite; "midstream components" such as cathodes, anodes, and electrolytes; and "downstream" of final assembly. A review of the supply chain for chips for artificial intelligence, identified the "upstream segment …[which] consist[s] mainly of silicon and boron…the midstream segment…[which] can be divided into three stages: design, fabrication, and assembly and packaging…[and]…the downstream segment of…distribution of finished chips for their various end-uses in cloud servers or edge devices." Damien Ma, Houze Song, Neil Thomas, "Supply Chain Jigsaw: Piecing Together the Future Global Economy," Paulson Institute, April 2020, 7, 15-16, https://macropolo.org/wp-content/uploads/2020/04/Supply-Chain.pdf

110 Thomas Y. Choi, Dale Rogers and Bindiya Vakil, "Coronavirus Is a Wake-Up Call for Supply Chain Management," *Harvard Business Review*, March 27, 2020, https://hbr.org/2020/03/coronavirus-is-a-wake-up-call-for-supply-chain-management.

111 Ibid. Lest a simplified description of supply chains makes the process seem somewhat straight forward: "In modern global value chains, production processes are often spread across dozens of firms operating in multiple countries. The average automobile, for instance, contains about 30,000 parts, and one recent analysis found Toyota relied on 2,192 distinct firms (both direct and indirect suppliers) in its production process." Geoffrey Gertz, "The Coronavirus Will Reveal Hidden Vulnerabilities in Complex Global Supply Chains," Brookings, March 5, 2020, https://www.brookings.edu/blog/future-development/2020/03/05/the-coronavirus-will-reveal-hidden-vulnerabilities-in-complex-global-supply-chains/.

112 Choi, Rogers and Vakil, "Coronavirus Is a Wake-Up Call."

Similarly, the DOD/interagency supply chain review, noted earlier in this report, took the efforts of three hundred people.[113] Despite the costs, the importance of such a review is illustrated by testimony on the limitations of the federal government's knowledge regarding pharmaceutical supply chains. In her October 2019 testimony, noted above, Dr. Woodcock stated that the FDA lacked reliable information about resilience of the pharmaceutical supply chain:

> "To answer this question, FDA would need to know… how much unused capacity exists in the US manufacturing base for APIs [active pharmaceutical ingredients]; how much additional API this capacity could supply within a given time period; how far this capacity would go in filling the gap between US patients' needs and the amount available if China or India, or another country, were to reduce or stop the supply to the US market; and how long would it take to increase production enough to meet patients' needs, and whether the financial investment would be sustainable for the pharmaceutical industry."[114]

Dr. Woodcock concluded that since these factors were unknown, "we cannot perform a reliable gap analysis."[115]

A "reliable gap analysis," as Dr. Woodcock suggests, is warranted for other key critical infrastructures. The sector-specific agencies will need to evaluate how best to accomplish this including whether, as a practical matter, such an effort might be limited to the most important firms selected for size, importance of product, or some other factor.

In undertaking such a review, government has two roles. First, Congress should provide the resources and support for the actual mapping of the supply chains, which, as noted above, are costly endeavors. Second, Congress should require that the sector-specific agencies integrate the results regarding individual companies and separate sectors into an overall view that gives a basis for an effective national approach. As one analysis stated:

> "Each firm has only a blinkered, incomplete view of its own little corner of global supply chains—governments must step in to piece together the bigger picture. A better mapping of supply chains will allow policymakers to proactively identify possible choke points in global economic networks, and work to lessen vulnerabilities and introduce strategic redundancies where needed."[116]

The net result will be the evaluation and subsequent assurance of the robustness of supply chains at the macro and micro/firm level. The information derived from the mapping required by resilience stress tests will allow development of government policies to alleviate supply chain risk.

One of the critical risk areas is the issue of cybersecurity resilience which is discussed in the next section.

3. Resilient Cybersecurity for Key Critical Infrastructures

The importance of establishing cyber resilience has been widely underscored. As one report stated: "There is a cybersecurity gap. Despite all efforts, adversarial cyberattacks are outrunning defender security improvements in technology, processes and education."[117]

As noted in several places above, Congress recently established the Cyberspace Solarium Commission which issued a comprehensive report in March 2020, and more recently added a new white paper entitled "Cybersecurity Lessons From the Pandemic."[118] There is no need to redo such an effort. What Congress could usefully do, however, is to focus on one critical area relevant to resilience not covered by the Cyberspace Solarium Commission, but which would be complementary to that commission's recommendations. Specifically, Congress should enact legislation leading to the following:

Cybersecurity resilient architectures should be developed and implemented for the key critical infrastructures of energy, finance, food, health, transportation, water, and the defense industrial base, with federal funding to support both the development and operation of such architectures.

113 Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, 2, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

114 *Safeguarding Pharmaceutical Supply Chains in a Global Economy*, US House Committee on Energy and Commerce, Subcommittee on Health, 116th Cong. (2019) (statement of Janet Woodcock, M.D., Director - Center for Drug Evaluation and Research, Food and Drug Administration), 7, https://www.fda.gov/news-events/congressional-testimony/safeguarding-pharmaceutical-supply-chains-global-economy-10302019.

115 Ibid.

116 Gertz, "The Coronavirus Will Reveal Hidden Vulnerabilities."

117 Franklin D. Kramer and Robert J. Butler, *Cybersecurity: Changing the Model, Atlantic Council*, April 2019, 1, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Cybersecurity-Changing_the_Model.pdf.

118 Cyberspace Solarium Commission, *Cybersecurity Lessons from the Pandemic*, May 2020, https://www.solarium.gov/public-communications/pandemic-white-paper.

The information and communications technology sector should be both a recipient of and a participant in building cybersecurity resilient architectures.

> "Cybersecurity resilient architectures should be developed … to organize and coordinate an integrated set of capabilities that will work as a system."

The essence of a cybersecurity resilient architecture is to organize and coordinate an integrated set of capabilities that will work as a system to provide effective cybersecurity.[119] The critical point is "integrated." Key elements of an integrated resilient architecture would include use of private sector cloud technology; zero-trust architecture to ensure effective access management; development of secure hardware capabilities; and machine-learning/artificial-intelligence-augmented cyber defenses. Effective resilient architectures will integrate these capabilities into a systemic approach. The architecture would need to be sufficiently flexible that advanced and emerging technologies could regularly be incorporated. Likewise, it must be structured to allow for continuous risk mitigation as adversaries change their methods of attack. While there would be commonality in terms of underlying capabilities, different key critical infrastructures will require somewhat different architectures.

Building cybersecurity resilient architectures is a technological task. In this context, Congress should enact legislation that would establish a framework for a research and development strategy that would lead to the creation of resilient architectures which key critical infrastructure providers could rely on. Broadly speaking, an effective development effort would utilize a combined public-private approach, engaging key elements of the federal government, the information and communications technology sector, and the critical infrastructures for whom the architectures would be developed, each of which has relevant expertise:

> "[C]apabilities will come from both the private sector and the government. The use of private-sector cloud technology, automation, and artificial intelligence can be key for the provision of cybersecurity…Additionally, appropriately using highly effective available technology from major government security agencies, including the Department of Defense and the intelligence community, may provide significant benefits to key [critical infrastructures] CIKR."[120]

In implementing the actual construction of a cybersecurity resilient architecture, close attention will need to be given to the vulnerabilities in the global software supply chain, as noted above, and steps need to be taken to reduce as much as possible the introduction of such vulnerabilities into a cybersecurity resilient architecture.[121] A focused effort on software supply chain security in the context of resilient architectures could "provide resources to developers as well as a framework to measure software supply chain security performance…opening the possibility that such measures could trickle down into the private sector and be enforced within segments of the technology marketplace."[122] An important aspect of "raising the cost of software supply chain attacks should center on providing the whole of industry…easy-to-use tools and well-defined reference implementations…that [generate] rigorous security."[123] Efforts should include "baseline security improvements in open-source security packages…given the wide dependence on open-source code in commercial and national security applications."[124]

Congress will need to evaluate how best to generate such a combined public-private effort. One possibility would be to recommend initiating the activity through the use of one or more "Grand Challenges," an approach that has been undertaken in other areas, including by the Defense

119 The concept of cybersecurity resilient architectures was set forth in an earlier report which discussed the need for more effective resilience in the cyber arena. The report recommended establishing a "Common Reference Architecture" that could provide the basis for "resilience architectures." Kramer and Butler, *Cybersecurity: Changing the Model,* 6, 17. A recent RAND report reaches the same conclusion, through focused on the DIB and unclassified information. See Gonzalez et al., Unclassified But Secure, RAND (2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4227/RAND_RR4227.pdf

120 Kramer and Butler, *Cybersecurity: Changing the Model*, 7. The federal government has valuable cybersecurity research and development underway by a number of agencies in addition to the Defense Department and the Intelligence Community including the Department of Homeland Security and the Department of Energy. See, e.g., US Department of Energy, "Cybersecurity Research, Development, and Demonstration (RD&D) for Energy Delivery Systems," accessed August 23, 2020, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and.

121 Herr, Lee, Loomis, and Scott, *BREAKING TRUST*.

122 Ibid., 26.

123 Ibid.

124 Ibid., 28.

Department.[125] Another approach would be "[i]dentification of such pilot programs as the Secretary [of Defense] considers may be required to improve the cybersecurity of the defense industrial base" as the FY2020 National Defense Authorization Act provides.[126] The Defense Department has recently "move[d] to facilitating the exchange of classified information remotely among users" and "'In the secret and top secret realm, we have kind of cracked how to do telework in that way,' [said] Lauren Knausenberger, chief transformation officer at the U.S. Air Force."[127] Although issues of scale remain,[128] such a capability could provide a valuable element for a resilient cybersecurity architecture. Alternatively, the sector-specific agencies could take the lead but utilize the capabilities of the Defense Department and the intelligence community as well as the private sector. Whatever method is utilized, there are good reasons not to narrow down too quickly—or perhaps ever—to only a single approach.

First, as noted, there will be requirements that differ among different key critical infrastructure sectors even if the underlying approach is consistent. Second, as has been shown in the space or electric and autonomous vehicle arena with several private firms adding capabilities, there are a variety of different approaches that may prove effective. Just as there is not a single way to build an effective fighter aircraft, there likely will prove to be alternative but effective cybersecurity approaches to building cybersecurity resilient architectures. Third, diversity of finished capabilities adds to resilience.

Congress should also consider, as part of its legislative process, recommendations as to how such a resilient architecture might be operated and resourced. With few exceptions, most businesses, including key critical infrastructure firms, are not expert cyber operators. Those that are, such as certain large financial firms or major defense firms, might prefer their own systems. For most, however, there is a need for outside expert capabilities in the cybersecurity arena, similar to the need for such outside capacities in other expert-driven areas. Just as businesses look to expert providers to meet needs—for example, financial—that are beyond their own core capabilities, resilient architecture providers would be relied on to provide effective cybersecurity. There is, of course, an existing sector of cybersecurity providers including companies offering single or several capabilities, managed service providers, and cloud companies.[129] Congress should take testimony and determine what market arrangements, including legal requirements and financial incentives, are necessary to encourage the development of an expert sector that will undertake effectively to operate integrated resilient architectures on behalf of key critical infrastructures. Just as businesses rely, for example, on banks and other financial institutions for the technical aspects of financial transactions, a conceptually similar approach to cybersecurity would have expert entities (perhaps with government certification) operate the cybersecurity systems for most clients.

> "Most businesses … are not expert cyber operators … [and] need … outside expert capability in the cybersecurity arena."

The costs of operating a cybersecurity resilient architecture also need to be considered as part of the Congressional review. Keeping in mind that the reason for developing resilient architectures for key critical infrastructures is to protect against a major cyberattack with national security implications, there are strong reasons to include those costs as part of the overall national security budget. Including the costs of operating cybersecurity resilient architectures for designated key critical infrastructure firms (perhaps those identified through resilience stress tests) could be underwritten by creating a line item in the federal budget. This could be included as part of the budget for the Department of Homeland Security or, alternatively, in the budgets of the sector-specific agencies. The budgetary support provided by the Congress in conjunction with cybersecurity for the 2018 elections provides the basic

125 US Department of Defense: Defense Advanced Research Projects Agency, "Prize Challenges," https://www.darpa.mil/work-with-us/public/prizes#:~:text=%20DARPA%20has%20launched%20a%20number%20of%20prize,8%20Spectrum%20Collaboration%20Challenge%20%28%202016-2019%29%20More%20.

126 National Defense Authorization Act FY 2020, Section 1648(e)(2)(B), https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf. The Defense Department has promulgated a series of cybersecurity requirements for Defense Industrial Base companies through the Cybersecurity Maturity Model Certification, but those provide objectives and not an architecture. C. Todd Lopez, "DOD to Require Cybersecurity Certification in Some Contract Bids," *Department of Defense News*, January 31, 2020, https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/.

127 Frank Konkel, "The Pandemic is Pushing the Pentagon Toward Classified Telework," Defense One, August 19, 2020, https://www.defenseone.com/threats/2020/08/pandemic-pushing-pentagon-toward-classified-telework/167837/.

128 Ibid.

129 See TAG Cyber, *Security Annual: Outlook For 50 Cyber Controls (2020 edition)*, https://www.tag-cyber.com/downloads/2020-TAG-Cyber-Annual.pdf.

model for such an effort.[130] Congress should also evaluate whether tax incentives or user fees might be incorporated into a resource strategy.[131]

B. A Strategic Framework for Health Sector Resilience and Biodefense

In the health and biological arena, there are five core elements that are key to building a strategic framework for future effective resilience. These are: 1) maintaining high levels of research and development funding on emerging and infectious diseases, including moonshot initiatives directed to critical health problems; 2) enhanced support for public health activities to increase the capacity for prevention of and response to pandemics and biological attack; 3) expanded utilization in the health arena of artificial intelligence through the establishment of trusted data bases available to researchers and analysts; 4) a national plan to respond to a pandemic that would be federally directed pursuant to a new "Stafford Act-plus" legislative mandate and which would be operationally effective at the federal, state, and local levels; and 5) expanded research and development, and planning to enhance resilience to biological attack.

1) High-Level Funding for Research and Development on Emerging and Infectious Diseases

As noted above, Congress has previously enacted multiple statutes focused on the health arena, including the problems of pandemics and epidemics. While the objectives have been clear, the amount of resources that had been made available did not generate the kind of major research and development results that could have limited the impact of the coronavirus. Before the recently expanded resources allocated by Congress to address the fallout from COVID-19, the FY2020 budget for the National Institute of Allergy and Infectious Diseases [NIAID] was $5.89 billion.[132] By contrast, the several statutes passed in response to the coronavirus have authorized over $9 billion for vaccines,[133] and "NIAID received a total of $1.532 billion from Congress to support our research."[134] Similarly, prior to the onset of the virus, the CDC FY2020 operating budget was $7.9 billion.[135] Legislation responding to the virus significantly increased the amount the CDC receives by an additional approximately $11 billion, the great bulk for "COVID-19 tests, [and to] conduct surveillance, trace contacts, and related activities."[136]

> "The fundamental question … is to determine how to achieve consequential benefits from significantly increased budgets focused on emerging and infectious diseases."

The increased funding for the ongoing effort is highly desirable. The fundamental question in looking to protect against future pandemics is to determine how to achieve consequential benefits from significantly increased budgets focused on emerging and infectious diseases.

Answering that question requires understanding with some granularity both the objectives of any appropriated funding as well as the capacities of the public and private

130 "The Cybersecurity 202: States Spent Just a Fraction of $380 Million in Election Security Money Before Midterms," *Washington Post*, April 5, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/05/the-cybersecurity-202-states-spent-just-a-fraction-of-380-million-in-election-security-money-before-midterms/5ca697b81b326b0f7f38f32b/.

131 As noted above, intellectual property theft by China is widespread and presents a significant threat to innovative US companies who may find that their intellectual property is stolen and used competitively against them. As described above, therefore, establishment of cybersecurity resilient architectures should be an important element of implementing resilience as part of US national strategy. And while the initial effort should focus on critical infrastructures, innovative firms likewise need the protection, as the example of the attacks against vaccine developers demonstrates. There will be very few businesses that can defend against the persistent campaigns by undertaken by China. The Resilience Commission, described below, should therefore recommend that the cybersecurity resilience architecture effort be extended throughout the private sector as much as is practicable.

132 National Institute for Allergy and Infectious Diseases, *Budget Appropriation for Fiscal Year 2020*, January 8, 2020, https://www.niaid.nih.gov/grants-contracts/budget-appropriation-fiscal-year-2020.

133 Kristin Jensen, "US to pay $1 billion to stock up on J&J's coronavirus vaccine," Biopharmadive, August 5, 2020, ("The U.S. government's ambitious Operation Warp Speed project has now awarded more than $9 billion to vaccine developers in an effort to secure access to a wide array of candidates."), https://www.biopharmadive.com/news/johnson-johnson-coronavirus-vaccine-us-supply-deal/582961/.

134 National Institute for Allergy and Infectious Diseases, "Supplemental Appropriations Bolster NIAID's COVID-19 Response," May 20, 2020, https://www.niaid.nih.gov/grants-contracts/supplemental-appropriations-covid-19.

135 Centers for Disease Control and Prevention, *FY 2020 Operating Plan*, February 11, 2020, https://www.cdc.gov/budget/documents/fy2020/fy-2020-cdc-operating-plan.pdf.

136 Centers for Disease Control and Prevention, "CDC in Action: Working 24/7 to Stop the Threat of COVID-19," June 22, 2020, https://www.cdc.gov/budget/documents/covid-19/CDC-247-Response-to-COVID-19-fact-sheet.pdf: "+ $720+ million to Epidemiology and Laboratory Capacity (ELC) grantees for coronavirus surveillance and disease tracking, including artificial intelligence (AI) technologies to improve detection and diagnosis of COVID-19
+ $750+ million for Urgent Response Needs for States, Localities, and Territories
+ $26+ million for Emerging Infections Program sites to enhance surveillance capabilities
+ $159 million to a new grant funding opportunity for tribes
+ $10.25 billion to develop, purchase, administer, process, and analyze COVID-19 tests, conduct surveillance, trace contacts, and related activities."

sectors to effectively and efficiently use such funds. On the theory that "ready, aim, fire" is better than "ready, fire, aim," Congress should require NIAID to develop a strategic plan that would create an effective multiyear approach, utilizing increased R&D resources by both the public and private sectors including the development of coordinated public-private partnerships. As part of its legislative process, Congress should receive expert testimony as to the appropriate areas of focus, including whether and which health challenges warrant a moonshot approach.

One leading expert has stated: "Of all the vaccines that deserve priority, at the very top of the list should be a 'universal' influenza vaccine, which would be game changing."[137] A variant of that approach recommends "design[ing] antiviral compounds that may have an effect against high-risk viral families [and which]...could...target a specific pathway shared by all family members in designated viral families."[138] A third area might be antimicrobial antibiotic research, the importance of which is illustrated by a group of pharmaceutical companies having recently pledged approximately $1 billion to support a fund. Their goal is "to bring two to four new antibiotics to patients by 2030 through collaboration between pharmaceutical companies, philanthropies, development banks, and multilateral organizations to reinvigorate and accelerate antibiotic development."[139] Another different suggestion is to "establish a global, genomic-based biosurveillance platform...[that would] enable a surveillance system that facilitates preemptive [actions] and rapid responses to outbreaks as well as early development of diagnostic pipelines and vaccine."[140] There are undoubtedly other areas that warrant review.

The United States has a significant number of top-ranked biomedical research entities including universities, non-profits, and the federal government itself. The private sector is likewise a highly valuable contributor.[141] The extraordinary number of efforts currently being undertaken to develop a vaccine for the coronavirus demonstrates that there is a great deal of capability that could be harnessed, given the right kind of incentives.[142] A five-year funding plan—or perhaps even a ten-year funding plan—with annual review would provide for the assurance of continued funding that is key to stable operations of public, private, and nonprofit research and development activities, while at the same time having sufficient flexibility to respond to changing circumstances.[143]

> "A [multi-year] funding plan ... would provide for the assurance of continued funding ... key to research and development activities."

2) Enhanced Support for Public Health Activities to Increase the Capacity for Prevention of and Response to Pandemics

The objectives of the United States public health system—"[k]eeping Americans safe from disease, disaster, and bioterrorism"[144]—are clear enough, but the reality is that "keeping Americans safe" has not been accomplished during the current pandemic. There needs to be an evaluation as to why this failure has occurred and how to be successful in the future. While the struggle against COVID-19 is still ongoing, the next administration as well as various committees of Congress will undoubtedly undertake to review that question. Additionally, however, Congress should charge the Resilience Commission, proposed below, with reporting on that question and offering its recommendations. The proposed commission, with membership incorporating executive, congressional, state and local, private sector, and academic perspectives, could undertake thorough factfinding and offer a bipartisan and expert perspective on the issues.

Whatever the review mechanisms turn out to be, from the start there needs to be a thoughtful review of the performance of the Centers for Disease Control and Prevention.

137 Osterholm and Olshaker, "Chronicle of a Pandemic Foretold."

138 "Recommendations for Improving America's Readiness for the Next Pandemic," Johns Hopkins Center for Health Security, June 30, 2020, 2, https://www.centerforhealthsecurity.org/news/center-news/pdfs/200630-PrepareforFuturePandemics-JHCHS.pdf.

139 Alex Keown, "Biopharma Giants Back Launch of AMR Fund with $1 Billion," BioSpace, July 10, 2020, https://www.biospace.com/article/pfizer-j-and-j-back-support-launch-of-amr-fund-with-100-million-pledges/.

140 W. John Kress, Jonna A. K. Mazet and Paul D. N. Hebert, "Opinion: Intercepting Pandemics Through Genomics," Proceedings of the National Academy of Science, June 23, 2020, https://www.pnas.org/content/117/25/13852.

141 Examples can be found at Nature Index, "The Nature Top 200 Institutions in Biomedical Sciences," 2019, https://www.natureindex.com/supplements/nature-index-2019-biomedical-sciences/tables/overall.

142 The estimates vary but cite well over 100 different research efforts and perhaps as many as 200. See Milken Institute, "COVID-19 Treatment and Vaccine Tracker," August 4, 2020, https://covid-19tracker.milkeninstitute.org/#vaccines_intro.

143 Senator Lamar Alexander has recommended a ten-year approach in a proposed bill and floor statement. See Senator Alexander Floor Remarks: Preparing for the Next Pandemic Act, July 20, 2020, https://www.help.senate.gov/imo/media/doc/Senator%20Alexander%20Floor%20Remarks%20Preparing%20for%20the%20Next%20Pandemic%20Act.pdf.

144 *Impact of Chronic Underfunding*, 6.

Critical questions—all of which are well-known to the public health community—regarding the preparedness of CDC to respond to a fast-moving pandemic include questions about: threat assessment and monitoring; data and surveillance capabilities; the utilization of artificial intelligence including the availability of relevant data bases; and the capacity to work effectively with state and local health authorities and providers.[145] Structural questions include whether the CDC is properly sized for responding to a pandemic, what should be the relationship between the CDC and the HHS assistant secretary for preparedness and response, and whether CDC needs greater authorities and/or independence. Making the CDC more effective is a critical element of being prepared for a future pandemic or biological attack.

A second and related critical issue is the question of funding, both at the federal and the state/local levels. The two are intertwined because, as noted earlier, "federal funds are the largest source of funding for state public health departments, with CDC being the single largest source of public health funding that flows to states, tribes, and territories."[146] As discussed above, there appears to be general agreement that public health activities have been significantly underfunded,[147] with one analysis concluding that "an annual infusion of $4.5 billion is needed to fully support core public health foundational capabilities at the state, territory, local, and tribal levels nationwide."[148]

"Congress should establish a substantially increased public health budget."

Congress should establish a substantially increased public health budget. While an additional $4.5 billion annually would be a large increase, it pales against the losses created by the coronavirus. Moreover, when looking at a pandemic as a security as well as a health issue, that level of funding would be entirely in keeping with other security measures included in the more than $700 billion national security budget.

A related issue is the need for a significant expansion of health sector personnel. The requirements are substantial: "[T]the United States could see an estimated shortage of between 54,100 and 139,000 physicians, including shortfalls in both primary and specialty care, by 2033."[149] This includes a deficit of 21,400 to 55,200 primary care physicians,[150] even as inadequate primary care has been a factor in the coronavirus' virulence, disproportionately affecting the less healthy. Moreover, future personnel deficits are not limited to doctors. As data from the Health Resources and Services Administration (HRSA) shows, the need goes beyond doctors to multiple "allied health professions" such as community health workers, emergency medical technicians and paramedics, medical and clinical laboratory technologists, and pharmacists.[151]

Within the public health sector itself, the workforce issues are similarly significant:

> "Reductions in federal and state public health budgets have undermined efforts to hire, train, and retain a strong public health workforce, which in turn limits governments' ability to effectively protect and promote the health of their communities. Over the last decade, local public health departments lost an estimated 56,360 staff positions due to federal, state, and local budget cuts."[152]

This is necessarily an issue for Congress to review and determine funding levels and other incentives necessary to ensure a satisfactorily sized public health workforce. Though if the proposed Resilience Commission is established, Congress could utilize it to undertake factfinding and present recommendations. One analysis recommended:

> "Congress should prioritize development of a public health workforce, including by issuing funding incentives to enter the public health workforce, such as offering loan repayments, recruiting and

145 See generally Id., 4.

146 Ibid., 10.

147 "CDC's budget remains inadequate to meet the nation's public health needs; [and] many states that need funding to support state and local public health initiatives do not get that funding because the demand outlasts the available resources." Ibid., 4.

148 Ibid., 8.

149 "New AAMC Report Confirms Growing Physician Shortage," Association of American Medical Colleges, June 26, 2020, https://www.aamc.org/news-insights/press-releases/new-aamc-report-confirms-growing-physician-shortage#:~:text=According%20to%20new%20data%20published,and%20specialty%20care%2C%20by%202033.

150 Ibid.

151 Health Resources and Services Administration, "Allied Health Workforce Projections," June 2019, https://bhw.hrsa.gov/health-workforce-analysis/research/projections/allied-health-workforce-projections.

152 *Impact of Chronic Underfunding*, 7.

> retaining a workforce with needed skills (such as informatics), and improving the training and curriculum for a modern public health workforce."[153]

A fourth issue is the need for upgrading technological capabilities:

> "The nation's public health surveillance infrastructure relies on antiquated, disconnected systems and methods for tracking and responding to diseases. Local, state, and federal data systems have not kept pace with current technologies and result in delayed detection and response to public health threats. Cross-cutting investments would revitalize CDC's data infrastructure, as well as shore up state and local public health surveillance capabilities."[154]

One estimate is that an adequate budget would be "$1 billion over 10 years to modernize the public health surveillance enterprise and to build secure, interoperable systems and a highly trained workforce."[155] Congress has already taken worthwhile steps in this area in the CARES Act by providing $500 million available until FY2024.[156] Congress could have the proposed Resilience Commission also review this issue including both the mechanisms and the amount of funding necessary to ensure that state and local systems are effectively modernized.

3) Expanded Utilization of Artificial Intelligence Through Development of Trusted Data Bases

Artificial intelligence (AI) capabilities are already significantly utilized in the health arena, but there are good reasons to expect that expanded use of these technologies will be of major value in preparing for and responding to future pandemics.[157] This application of AI is of particular value given the increasing availability of data: "With the amount of medical data in the world now estimated to double every couple of months or so, health care was ripe for AI—even before the virus struck."[158]

Artificial intelligence is already being utilized in the context of the current pandemic. As an example:

> "In the UK, biotech company BenevolentAI turned its formidable artificial intelligence machine—set up to discover and develop new drugs—towards understanding the novel infection, then called 2019-nCoV. The company used its 'knowledge graph,' a large repository of medical information including connections extracted from scientific literature by machine learning, to look for existing medicines that could move quickly into clinical trials. AI enables it to solve pharmacological puzzles much faster than human experts."[159]

> "Expanded use of artificial intelligence could … broade[n] research … [and] surveillance capabilities, and reduc[e] the time necessary for the development of safe vaccines."

Another example shows the potential for AI to help with surveillance requirements relevant to responding to pandemics:

> "On New Year's Eve of [2019], the artificial intelligence platform BlueDot picked up an anomaly. It registered a cluster of unusual pneumonia cases in Wuhan, China. BlueDot, based in Toronto, Canada, uses natural language processing and machine learning to track, locate, and report on infectious disease spread. It sends out its alerts to a variety of clients, including health care, government, business, and public health bodies. It had spotted what would come to be known as Covid-19, nine days before the World Health Organization."[160]

153 Ibid., 25-26.

154 Ibid., 25.

155 Ibid.

156 Ibid.

157 "Deep learning—the capability to process massive, multi-model data at high speeds—presents one of the most far reaching opportunities for AI. Deep neural networks, a subtype of AI, have already been used to produce accurate and rapid algorithmic interpretation of medical scans, pathology slides, eye exams, and colonoscopies. [One can] see a clear roadmap of how AI, accelerated by the pandemic, will be infused into health care." "Covid-19 Will Accelerate the AI Health Care Revolution," *Wired*, May 22, 2020, https://www.wired.com/story/covid-19-will-accelerate-ai-health-care-revolution/.

158 Ibid.

159 Clive Cookson, "Biotechs Harness AI in Battle Against Covid-19," *Financial Times*, May 24, 2020, https://www.ft.com/content/877b8752-6847-11ea-a6ac-9122541af204.

160 "Covid-19 Will Accelerate."

As the above examples suggest, expanded use of artificial intelligence could have multiple benefits when responding to a pandemic. These include broadening research capabilities, enhancing surveillance capabilities, and reducing the time necessary for the development of safe vaccines and other medical treatments. However, as each of the examples further demonstrate, a critical issue for effective use of AI is having the relevant data necessary for analysis.

To be useful, data will need to be collected in a timely fashion and properly organized. Not all data is equally useful to each different task. Data relevant to discovering new drugs will be different than data relevant to monitoring during an ongoing pandemic. For some types of problem sets—game playing, for example—an AI algorithm can generate its own data, but access to real world data is critical for dealing with health issues.

Accordingly, a key task for dealing with future pandemics—both from the prevention and the response perspectives—is to establish, maintain, and continuously upgrade the data bases that are required for the different tasks.

Congress has previously established the National Security Commission on Artificial Intelligence (the AI Commission) "to consider the methods and means necessary to advance the development of artificial intelligence, machine learning, and associated technologies to comprehensively address the national security and defense needs of the United States."[161] The AI Commission has already issued several reports,[162] is analyzing a full spectrum of issues including data questions, and its members have recently focused on a number of issues specific to the pandemic.[163] One important report by a commissioner and staff members has a series of recommendations as to potential uses of artificial intelligence for pandemic response and preparedness.[164] Congress should utilize the capabilities of the AI Commission and request that the commission recommend—as the report by the one commissioner and staff does[165]—a framework that would ensure the establishment, organization, and usage of data sets relevant to the prevention, preparation for, and response to a pandemic. As the AI Commission is already well aware, in doing so, the commission will not be working on an empty canvas. The healthcare field has many existing data sets available to researchers,[166] and in the context of the pandemic there are multiple additional actions underway to create relevant databases for analysis by artificial intelligence. For example:

> "Kaggle, a machine learning and data science platform, is hosting the Covid-19 Open Research Dataset. CORD-19, as it is known, compiles relevant data and adds new research into one centralized hub. The new data set is machine readable, making it easily parsed for AI machine learning purposes. As of publication, there are more than 128,000 scholarly articles on Covid-19, coronavirus, SARS, MERS, and other relevant terms."[167]

Other data sets have likewise been utilized effectively in connection with the pandemic:

> "Researchers at Birmingham City university have adapted a neural network called DeTraC (short for decompose, transfer and compose) to detect Covid-19. Early experimental results showed that DeTraC could detect Covid-19 cases from an image data set collected from several hospitals around the world. It achieved 95 per cent accuracy in distinguishing Covid-19 X-rays from comparable images of other lung diseases."[168]

Looking to the future, it will be important to determine how to ensure that relevant data sets are built, maintained, and continuously upgraded, and that researchers and analysts can receive appropriate timely access to relevant data. Three challenges need to be resolved: first, organizing and maintaining the data for researchers and analysts to access, which involves developing appropriate repositories and models; second, ensuring security measures for the data that allow functionality of use while maintaining privacy of personal information; and, third, obtaining useful data in a timely fashion which, in the context of a pandemic, involves testing and other forms of collection.

As noted above, the amount of medical data is rapidly increasing. The AI Commission should evaluate which types of data bases are potentially most useful to the prevention of and response to pandemic disease, and identify those

161 "About," National Security Commission on Artificial Intelligence, https://www.nscai.gov/about/about.

162 E.g., National Security Commission on Artificial Intelligence, *Second Quarter Recommendations*, 2020, https://drive.google.com/file/d/1hgiA38FcyFcVQOJhsycz0Ami4Q6VLVEU/view.

163 White Paper Series on Pandemic Response and Preparedness included with Ibid.

164 Matheny, Zetter, deBlanc-Knowles, and Garris, *The Role of AI Technology*.

165 Ibid., p.21.

166 See one list at Research and Writing Guides, "The top list of research databases for medicine and healthcare," Paperpile, 2018), https://paperpile.com/g/research-databases-healthcare/.

167 "Covid-19 Will Accelerate."

168 Cookson, "Biotechs Harness AI in Battle Against Covid-19."

not already being undertaken as well as those in need of, or that would benefit from, support. The AI Commission should recommend actions to ensure the development of the needed data bases and should analyze how to establish in advance comprehensive open data sources without having to develop them on an ad hoc basis as has been the case for the Open COVID-19 Data Working Group effort.[169] One question will be which data bases the government needs to establish, and which might be in the private sector or in a shared public-private form.[170]

Public-private collaboration can be very effective. For example, "the White House and a coalition of leading research groups…prepared the COVID-19 Open Research Dataset (CORD-19."[171] Likewise, both CEPI and Gavi offer somewhat different models for public-private collaboration. The AI Commission should evaluate which approaches in which contexts would be effective for collecting, organizing, and making data available to researchers and analysts. The commission should also evaluate the "Johns Hopkins University epidemiologist Caitlin Rivers' argument that the coronavirus pandemic has made it clear that one crucial innovation we need is a new kind of institution…a 'center for epidemic forecasting'…where we have reliable forecasts that inform our everyday lives as the public, and also help decision makers to understand how best to respond to these outbreaks."[172]

The second data issue for the AI Commission involves the related questions of security and privacy. Data related to health is often both highly personal and highly regulated under the Health Insurance Portability and Accountability Act. Wherever health data bases are maintained that include personal health information, building a trusted data system that can be valuable for usage but can also protect such personal information is a necessary requirement. This is, of course, an issue that has received extensive attention, including from the HHS Office of the National Coordinator for Health Information Technology. That office has undertaken a variety of efforts, such as the draft Trusted Exchange Framework, to enhance secure usage of health data.[173] The AI Commission has already issued work by several of the commissioners relevant to the questions of privacy and security,[174] and is well-positioned to make appropriate recommendations.

Technology can be a key factor in achieving a satisfactory resolution. One worthwhile analysis discussed different security approaches currently in development that would allow for widespread usage of data by researchers while simultaneously protecting privacy. These include highly technical capabilities and related issues such as anonymization, pseudonymization, the risks of re-identification, decentralized data and federated machine learning, differential privacy, homomorphic encryption, and secure multi-party computation.[175] Keeping in mind, however, that the objective is not technical analysis but rather the creation of a strategic framework, an appropriate approach for the AI Commission would be to recommend the establishment of a research and development program for security capabilities that could link effective data collection and maintenance with desired privacy requirements.[176]

One such approach would be "the implementation of a data trust for medical and health-related information, as envisioned by the GeoTech Center" at the Atlantic Council.[177] The trust would be built on the types of technological tools noted above so that "researchers could access hard data

169 See Allen Institute For AI and 8 collaborators, "COVID-19 Open Research Dataset Challenge (CORD-19)," https://www.kaggle.com/allen-institute-for-ai/CORD-19-research-challenge.

170 The federal government does maintain health data bases, and could do more as one expert group has recommended: "The US government should create a central repository for serosurveys [antibody studies], similar to clinicaltrials.gov, which would be useful for SARS-CoV-2, but also for public health research on emerging viruses in the future." "Recommendations for Improving," 11.

171 Allen Institute for AI and eight collaborators, "COVID-19 Open Research."

172 Stephen Johnson, "How Data Became One of the Most Powerful Tools to Fight an Epidemic," *New York Times*, June 10, 2020, https://www.nytimes.com/interactive/2020/06/10/magazine/covid-data.html; see Caitlin Rivers and Dylan George, "How to Forecast Outbreaks and Pandemics," *Foreign Affairs*, June 29, 2020, https://www.foreignaffairs.com/articles/united-states/2020-06-29/how-forecast-outbreaks-and-pandemics.

173 Official Website of The Office of the National Coordinator for Health Information Technology (ONC), "Trusted Exchange Framework and Common Agreement," https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement.

174 Dr. Eric Horvitz, Hon. Mignon Clyburn, Dr. José-Marie Griffiths, and Dr. Jason Matheny, Privacy and Ethics *Recommendations for Computing Applications Developed to Mitigate COVID-192*, 2020), https://drive.google.com/file/d/1m0AT21dS2XJ6JIGMgo7SuLSLveWIO8WK/view.

175 Georgios A. Kaissis, Marcus R. Makowski, Daniel Rückert and Rickmer F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence*, June 2020, https://www.nature.com/articles/s42256-020-0186-1.pdf.

176 Simply to illustrate the technological potential: federated learning technology makes it possible for AI algorithms to gain experience from a vast range of data located at different sites. Nicola Rieke, "What Is Federated Learning?" NVIDIA, October 13, 2019, https://blogs.nvidia.com/blog/2019/10/13/what-is-federated-learning/. One discussion recognizes "the key issues of privacy and data protection, particularly when it comes to patients' records," and proposed "using federated learning…[so that] patients' data is stored and never leaves their host health system or hospitals or personal devices, as machine learning models are trained from separate datasets, processed and combined subsequently." "Covid-19 Will Accelerate." "Technologies, such as federated learning, homomorphic encryption, and trusted hardware execution environments…[can be combined to] ensure data is computed, transmitted, and stored to meet preferred [privacy] settings, as privacy requirements vary around different countries and cultures." Ibid.

177 Henry Westerman,*"Event recap: Increasing resilience by assuring trust in medicine, credentials, and supply chains," Atlantic Council,* July 12, 2020, https://www.atlanticcouncil.org/commentary/event-recap/event-recap-increasing-resilience-by-assuring-trust-in-medicine-credentials-and-supply-chains/.

while the studied individuals remain certain that their privacy is not compromised."[178] To assure privacy and control, the "data trust system [would be] developed by a coalition of public, private, and [non-governmental organization] NGO partners and maintained by citizen-juries [with] transparent regulations…[governing] medical researchers and practitioners and patients."[179] Security would be enabled by technology; privacy would be secured by "enabl[ing] individuals to take ownership of their data, deciding how and by whom it can be used."[180]

The third challenge to establishing relevant data sets is obtaining useful data in a timely fashion. This requires establishing and maintaining an organized system for collection and reporting of data—or perhaps more accurately a system of systems—running from localities to the states to the federal government. Given the multijurisdictional nature of this requirement, no single entity has the full jurisdictional competence over its resolution. Congress should, however, establish a federal framework that provides technical and resource support to states and localities to ensure the collection and reporting of data. As one expert group has stated, "Federal, state and local public health agencies need to be better equipped to capture, analyze, and display laboratory, clinical, and other data in a timely manner. This will require having new data sharing agreements with and between government agencies, clinical and laboratory and other private sector data providers, stronger information technology systems to access and store data, and robust, inhouse data analytic capabilities."[181]

In the context of a pandemic, obtaining near real-time data is necessary for rapid and effective analysis and response. The key to obtaining such data is a reliable and timely testing program: "Testing data are needed to manage all aspects of a pandemic. For instance, they are a cornerstone of epidemic forecasting models, which are sorely needed to reveal the future demand for care, including the timing of case surges and the magnitude of required emergency medical services, hospital staff, hospital beds, ventilator equipment, and mortuary services."[182]

As the difficulties with undertaking testing in the current pandemic have shown, however, the "United States has underfunded and undermined its disease surveillance programs and done a poor job of organizing its 50 state systems for collecting and reporting testing data. The pandemic affects all states, yet states' data are incomplete and uneven at best."[183]

Congress should receive expert testimony regarding the efficacy of multiple testing methods[184] in order to establish a framework for an effective and funded testing system that will operate through coordinated federal, state, and local governmental efforts, and engage public and private health entities and providers.

Data bases and testing will be of little value, however, if there is not a national plan to respond to a pandemic. That is the subject of the next section.

4) National Plan to Respond to a Pandemic or Biological Attack

In responding to future pandemics, the United States needs a much more effective set of operational capabilities than has been available in dealing with the coronavirus. On paper, many, if not all, of these capabilities exist. As noted above, the National Security Strategy discusses pandemics and resilience. The National Response Framework states that it "provides foundational emergency management doctrine for how the Nation responds to all types of incidents;"[185] and Emergency Support Function (ESF) #8—Public Health and Medical Services Annex is intended to provide a framework for health emergencies.[186] The Department of Health and Human Services has

178 Ibid.

179 Ibid.

180 Ibid.

181 "Recommendations for Improving," 5.

182 Eric C. Schneider, M.D., "Failing the Test — The Tragic Data Gap Undermining the U.S. Pandemic Response," *New England Journal of Medicine*, May 15, 2020, https://www.nejm.org/doi/full/10.1056/NEJMp2014836.

183 Ibid.

184 See Johnson, "How Data Became." Testing methods range from direct testing of symptomatic individual individuals to the use of artificial intelligence and include activities such as sentinel surveillance—widespread, early-stage testing in critical populations that may be at risk; syndromic surveillance, which involves data tracking the appearances of disease symptoms before they get to a doctor or a hospital, for example by collecting information through internet-connected thermometers; and sewage sampling, "because many dangerous pathogens are expelled in human waste, sewage samples are the most direct way of surveying viral or bacterial activity in a given community — short of testing people directly." Ibid. See also Matheny, Zetter, deBlanc-Knowles, and Garris, *The Role of AI Technology*, 25.

185 US Department of Homeland Security, *National Response Framework Fourth Edition*, October 28, 2019, ii, https://www.fema.gov/media-library-data/1582825590194-2f000855d442fc3c9f18547d1468990d/NRF_FINALApproved_508_2011028v1040.pdf.

186 US Department of Homeland Security, *National Response Framework, Emergency Support Function #8 – Public Health and Medical Services Annex*, https://www.fema.gov/media-library-data/20130726-1825-25045-8027/emergency_support_function_8_public_health___medical_services_annex_2008.pdf.

established an HHS Concept of Operations for ESF #8,[187] and the Pandemic Influenza Plan[188] states that "the capacity and capabilities developed for pandemic influenza preparedness will enable HHS to respond more effectively to other emerging infectious diseases."[189]

As the responses to the coronavirus demonstrate, however, moving from descriptions on paper to actual operations has proved very difficult.[190] There needs to be a much more effective system.

> "Congress needs to legislate … a 'Stafford Act-plus' that puts the federal government in charge if a pandemic or comparable event has occured."

First, the federal government needs to take a more directive role in the event of a future pandemic. Inasmuch as the impact and consequences of a pandemic are nationwide and effective response requires coordinated efforts throughout the nation, a federally directed approach is required. By contrast, the current system operates generally under the framework established by the Stafford Act which requires states to request federal assistance and is more oriented to a localized problem than a nationwide emergency:

> "In the United States, the principles of disaster management presume a leadership role by the local, state, territorial, and tribal governments affected by the incident. The U.S. federal government does not automatically provide assistance when a disaster occurs. Instead, the federal government provides coordinated, supplemental resources and assistance only if requested and approved."[191]

With a pandemic, a coordinated national response that is undertaken immediately is critical to establishing an effective, resilient response. To be sure, states and localities will nonetheless have much to do, so their engagement needs to be evaluated to ensure productive coordination. Likewise, critical infrastructures will need support but also to be supporting entities. However, given the importance of a national response to a pandemic, the authorities required for a federally directed approach need to be analyzed and appropriate legislation needs to be adopted. Congress needs to legislate the changes in authorities that would be necessary to create an effective federally directed and coordinated approach for federal/state/local/critical infrastructure interactions in the context of a nation-wide emergency—in effect to legislate a "Stafford Act-plus" that puts the federal government in charge if a pandemic or comparable event has occurred.

Second, Congress needs to determine what will be required for HHS to have an effective operational capability in the face of a pandemic. Undoubtedly, this issue will come under scrutiny in the next administration and in hearings in the Congress, but the proposed Resilience Commission could present a useful bipartisan, expert set of recommendations.

An operational capability that is nationwide in scope will require both more extensive federal personnel as well as highly coordinated efforts with state and local governments and the private sector. There needs to be a thorough evaluation of the planning and necessary resources:

> "Even before a specific threat has arisen, a broad group of actors should be brought together to develop a comprehensive strategy—with enough built-in flexibility that it can evolve as conditions demand—and then they should repeatedly review and rehearse it. That effort should involve everyone from high-level government and public health officials to emergency responders, law enforcement, medical experts and suppliers, food providers, manufacturers, and specialists in transportation and communications. (As emergency

187 US Department of Health and Human Services, *HHS Concept of Operations for ESF #8*, https://www.phe.gov/Preparedness/planning/mscc/handbook/chapter7/Pages/hhsconcept.aspx.

188 US Department of Health and Human services, *Pandemic Influenza Plan, 2017 Update*, https://www.cdc.gov/flu/pandemic-resources/pdf/pan-flu-report-2017v2.pdf.

189 Ibid. 3.

190 One analysis of what should have been done stated: "Even with the lack of long-range planning and investment, there was much that the US government could and should have done by way of a short-range response. As soon as the novel and deadly coronavirus was identified, Washington could have conducted a quick but comprehensive review of national PPE [personal protective equipment] requirements, which would have led to the immediate ramping up of production for N95 masks and protective gowns and gloves and plans to produce more mechanical ventilators. Relying on the experience of other countries, it should have put in place a comprehensive test-manufacturing capability and been ready to institute testing and contact tracing while the number of cases was still low, containing the virus as much as possible wherever it cropped up. It could have appointed a supply chain coordinator to work with governors, on a nonpartisan basis, to allocate and distribute resources." Osterholm and Olshaker, "Chronicle of a Pandemic Foretold."

191 Congressional Research Service, *Congressional Primer on Responding to and Recovering from Major Disasters and Emergencies*, June 3, 2020, https://fas.org/sgp/crs/homesec/R41981.pdf.

> planners are fond of saying, you don't want to be exchanging business cards at a disaster site.) The strategy should offer an operational blueprint for how to get through the one or two years a pandemic would likely last."[192]

Among other requirements, pandemics will call for a surge capability well beyond that required for more localized operations.[193] As part of creating a Health Sector Base, discussed further below, HHS and Congress should evaluate how best to accomplish that high level of capacity. This will require a review of the "require[d] coordination across the healthcare system to ensure an adequate supply of staff; hospital beds, including intensive care beds; personal protective equipment; medicines; and ventilators. While preparedness standards exist for individual facilities through the Centers for Medicare and Medicaid Services (CMS) and The Joint Commission, systemwide readiness requires external coordination and planning."[194]

One proposal concluded that to achieve the necessary level of capability, new authorities in the form of a new regulatory approach would be required: "Congress and HHS should work to build surge capacity across the system by establishing an external regulatory body to set, validate, and enforce standards for healthcare facility readiness, stratified by facility type, with authority to impose financial penalties."[195] Whether a new external body is required or not, there is no doubt that under a Stafford Act-plus legislative mandate for nation-wide emergencies, significant new regulation and its authorization by Congress will be a necessary component.

Third, a pandemic plan should be built, exercised and trained for in order to generate a far better result than has occurred with respect to the coronavirus pandemic. As one expert has pointed out, multiple factors combine to add to the difficulty of planning for a pandemic:

> "Despite the complexity, [it is important to] consider in [the] plan the combination of [t]he direct impact of [the pandemic] on the population, [t]he collateral damage from a potentially collapsing global just-in-time economy, [t]he lack of comprehensive business continuity planning, [and] [t]he inability of governments around the world to provide exhaustive and immediate relief."[196]

Given the need for national and local engagement in any effective response, both top-down and bottom-up planning, training, and exercising will be necessary. It is especially important to engage at the local level since that is where most interfacing with the public takes place, and it will be equally important to plan with critical infrastructures, such as the electric grid and the food industry, that will need to operate effectively despite a pandemic.[197] The Department of Homeland Security undertakes and supports a variety of exercises, but those efforts have not provided a basis for a coordinated response to the coronavirus and need to be further evaluated and revised. Additionally, how to best utilize the capabilities of the National Guard and those that the Defense Department brings through its Defense Support to Civilian Agencies is another issue, as is the effective use of the National Disaster Medical System,[198] and how best to use volunteer capabilities as in the Medical Reserve Corps.[199]

The best planning capabilities in the federal government exist at the Department of Defense, and the DOD's Northern Command has a mandate to support homeland security. DOD does not have the same substantive expertise as HHS, however. Further, DHS needs to be engaged. Accordingly, Congress should require the establishment of a Joint Interagency Task Force (JIATF) that will undertake the establishment of the necessary planning, exercising, and training. Congress should further require regular reporting and testimony as to the effectiveness of the JIATF efforts.

192 Osterholm and Olshaker, "Chronicle of a Pandemic Foretold."

193 See Lawrence O. Gostin, "The Great Coronavirus Pandemic of 2020—7 Critical Lessons," JAMA Health Forum, August 13, 2020, ("Resilient health systems require surge capacity to cope with health emergencies in the event hospitals become overrun."), https://jamanetwork.com/channels/health-forum/fullarticle/2769600.

194 Trust for America's Health, *What we are learning from COVID-19 about being prepared for a public health emergency*, May 2020, 4, https://www.tfah.org/wp-content/uploads/2020/05/TFAH2020CovidResponseBriefFnl.pdf.

195 Ibid.

196 Michael Osterholm, **"**The Fog of Pandemic Planning," University of Minnesota Center for Infectious Disease Research and Policy, January 31, 2007, https://www.cidrap.umn.edu/news-perspective/2007/01/fog-pandemic-planning.

197 An example of the type of exercise that engages both federal and local officials as well as the private sector are the so-called Jack Voltaic exercises which focused on combined natural disaster and cyberattack scenarios. Army Cyber Institute, "Executive Summary," *JACK VOLTAIC 2.0 Threats to Critical Infrastructure*, 2018, https://www.afcea.org/event/sites/default/files/files/JackVoltaic_ExecSummary_R12%20(Final).pdf.

198 Recently the subject of a report by the General Accountability Office stating that improvement is warranted. Government Accountability Office, *Public Health Preparedness: HHS Should Take Actions to Ensure It Has an Adequate Number of Effectively Trained Emergency Responders*, June 2020, https://www.gao.gov/assets/710/707710.pdf.

199 "The Medical Reserve Corps (MRC) is a national network of volunteers, organized locally to improve the health and safety of their communities. The MRC network comprises approximately 175,000 volunteers in roughly 850 community-based units." Another potentially useful suggestion would be scaling up AmeriCorps, for example, as contact tracers. Michael Tubbs and Emma Vadehra, "Scale up AmeriCorps," *Washington Post*, April 30, 2020, https://www.washingtonpost.com/opinions/2020/03/20/coronavirus-is-upending-society-here-are-ideas-mitigate-its-impact/?arc404=true#Tubbs-Vadehra.

> "Congress should require the establishment of a Joint Interagency Task Force … [for pandemic] planning, exercising, and training."

Fourth, with respect to the Strategic National Stockpile, Congress should require that the federal government undertake to regularize an appropriate level of inventory, ensuring through contracting with manufacturers that there are sufficient materials on hand. As noted above, a number of efforts are currently underway, particularly by the DOD using authorities under the Defense Production Act. These should be maintained over time to ensure the stockpile's capacity. However, there will be judgment calls to be made to determine how much should be maintained in the stockpile and how much reliance should be based on a manufacturing surge capability Additionally, to make the stockpile most effective, logistic arrangements should be mapped out and practiced so that key materials can promptly be transported to where they are required. Congress should require regular reports on the status of the stockpile to ensure that the necessary actions are being taken.

Fifth, Congress should require the establishment of a Health Sector Base as one of the Resilient Industrial Bases discussed above. The need for a high degree of readiness in a Health Sector Base is well-established:

> "The COVID-19 pandemic has made crystal clear the importance of a well-resourced and well-run medical countermeasure enterprise. A robust medical countermeasures program consists of the research, development, stockpiling and distribution of medical supplies, drugs, devices, vaccines and other products for use in emergencies. The U.S. must have the surge capacity to be able to facilitate the rapid development and procurement of diagnostic tests and personal protective equipment (e.g., gloves, respirators, goggles, face shields, and gowns), therapeutics, and vaccines—and then distribute them strategically and equitably."[200]

One analysis also focused on the need for developing ways to immunize the population "within days to weeks, rather than months," and recommended that "Funding or other incentives should be provided to enable the development of manufacturing infrastructure for particularly promising administration technologies."[201]

As the foregoing suggests, in analyzing how to develop a Health Sector Base, Congress should require that HHS recommend how much manufacturing capability for health materials should be maintained—and, if necessary, expanded—in the United States and/or with reliable allies and partners.

However, one significant and necessary change is clear. A great deal of medical material and pharmaceuticals are currently produced in China, which cannot be counted on as a reliable source. Therefore, the United States should, at a minimum, have a "China plus one" approach to sourcing for critical health requirements. It should be recognized that ensuring such a plus-one capacity of an additional country source may create costs that could be substantial. The plus-one country might be the United States, or it might be a reliable ally or partner. Plus one could also mean plus two or more. The federal government might well have to utilize guaranteed "take-off contracts" and similar contractual efforts to ensure "plus one" companies have an appropriate market for their products as well as for maintaining the necessary excess production capability required for any ramp-up. Congress should enact the necessary legislation to authorize and fund such efforts.

Finally, inasmuch as a pandemic is a global event, there is an obvious need for an international effort to complement homeland resilience. International efforts have received attention from many analyses, including a recent Atlantic Council report which describes a number of initiatives that, if adopted, would strengthen the capacity of nations working together.[202] Achieving those ends will require significant international diplomacy. This report is focused on resilience in the United States, but a comprehensive analysis of international health requirements is equally warranted.

5. Resilience and Biodefense

Biodefense encompasses the full spectrum of preparation and response to both naturally occurring diseases and deliberate adversarial attacks by nation states or non-state

200 *What We are Learning from COVID-19 About Being Prepared for a Public Health Emergency*, Trust for America's Health, May 2020, 3, https://www.tfah.org/wp-content/uploads/2020/05/TFAH2020CovidResponseBriefFnl.pdf.

201 "Recommendations for Improving," 7.

202 Jeffrey Cimmino, Rebecca Katz, Matthew Kroenig, Josh Lipsky, and Barry Pavel, *A Global Strategy for Shaping the Post-COVID-19 World*, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/AC-A-Global-Strategy-for-Shaping-the-Post-COVID-19-World.pdf.

actors.[203] This section of the report focuses on the latter of those threats.

As was described earlier in the report with respect to the ostensible capacity to respond to a pandemic, there similarly exists a bureaucratic structure with the mission of preparing for and responding to an adversarial biological attack. In addition to the promulgation of the National Biodefense Strategy itself, a presidential executive order issued in 2018 created the Biodefense Steering Committee chaired by the secretary of Health and Human Services and including the departments of State, Defense, Justice, Agriculture, Veterans Affairs, Homeland Security, and the Environmental Protection Agency.[204] Multiple departmental components are engaged. The HHS relevant entities include the assistant secretary for preparedness and response, the CDC, and the Strategic National Stockpile. The Department of Homeland Security's Countering Weapons of Mass Destruction Office has a mission to prevent, and promote readiness for responding to, biological threats.[205] That office operates the DHS BioWatch Program "[which] provides early warning of a bioterrorist attack in more than thirty major metropolitan areas across the country."[206] At the Department of Defense, commands and agencies relevant to resilience against an adversarial biological attack include Northern Command, the Joint Staff, the Defense Threat Reduction Agency, the Defense Advanced Research Projects Agency, and the Army Medical Research Institute of Infectious Diseases. In short, there is no deficiency of responsible agencies, at least not on paper.

As is true in the health sector more generally, however, the multiplicity of entities does not mean that there is actually an effective operational program to respond to an adversarial biological attack. The core elements needed to run such a program are clear enough. The required capabilities have much in common with those needed to deal with naturally occurring diseases, as discussed in the section on health sector resilience above, and have long been understood. For example, a 1999 analysis described the following:

> "Early detection capability is an essential tool in cases of suspected uses of biological weapons. The sooner a bioterrorist attack is detected, the faster the medical community can respond to prevent additional exposure and to begin treatment of those who have been exposed."
>
> "Rapid epidemiological investigation to identify the nature of the disease outbreak will be critical for limiting casualties in the event of a bioterrorist attack. Coordinated efforts between local and regional clinical public health laboratories and sophisticated diagnostic laboratories at the FBI, CDC, and USAMRIID [US Army Medical Research Institute of Infectious Diseases] will also be critical."
>
> "[While] [e]ffective vaccines and antitoxins exist for several of the agents most likely to be used in a biological weapons attack, [a]dditional vaccines and new therapies are needed."
>
> "For the general public, there are currently insufficient supplies of medicinals and trained personnel to cope with a terrorist use of biological weapons. Public health officials have been calling for the stockpiling of antidotes, antimicrobials, and vaccines that could be used in the event of a biological weapons attack and for the development of new medical treatments for diseases caused by biological weapons agents."
>
> "[T]he real front line of defense will be the medical and public health community. To minimize the effects of a biological terrorist attack, health care professionals and public health authorities must…have an understanding of the agents that bioterrorists might use, especially of the different effects that may result from exposure by various routes."[207]

The written analysis set forth in the 2018 National Biodefense Strategy demonstrates that the federal government is intellectually aware of the requirements described, but, as the response to the coronavirus has made clear, no effective strategy has actually been operationalized and implemented. In that regard, it is worth noting that the 2018 strategy has been preceded by similar efforts in prior

203 There could also be consequences from an accidental release into the environment.

204 The White House, *Presidential Memorandum on the Support for National Biodefense*, September 18, 2018, section 2(c), https://www.whitehouse.gov/presidential-actions/presidential-memorandum-support-national-biodefense/.

205 US Department of Homeland Security, Countering Weapons of Mass Destruction Office, https://www.dhs.gov/countering-weapons-mass-destruction-office.

206 US Department of Homeland Security, "Detecting Bioterrorist Attacks," https://www.dhs.gov/biowatch-program.

207 Ronald M. Atlas, "Combating the Threat of Biowarfare and Bioterrorism: Defending Against Biological Weapons is Critical to Global Security," BioScience, Volume 49, Issue 6, June 1999, 465–477, https://academic.oup.com/bioscience/article/49/6/465/229529.

administrations[208] but, notwithstanding the broadly consistent policy direction over a number of years, the level of actual capabilities has not significantly improved.

The 2018 strategy does set forth an "Implementation Plan,"[209] but its goals are general and moving from thoughts on paper to effective programs has proved difficult. As a result, there are multiple deficiencies. For example, Dr. Asha M. George, executive director of the Bipartisan Commission, testified in October 2019:

> "Given the severity of the threat, the federal government has spent, and continues to spend, millions to develop, improve, and deploy technology in hopes of rapidly detecting biological attacks… Unfortunately,…the equipment designed to detect airborne biological contaminants do[es] not perform well and have not progressed significantly since their initial deployments. The federal government has also failed to efficiently and comprehensively integrate and analyze…surveillance data."[210]

Similarly, Dr Jennifer L. Rakeman, assistant commissioner and laboratory director of the New York City Department of Health and Mental Hygiene, testified:

> "A biodetection program is an essential public health tool…However, both [the current] BioWatch and the proposed BD21 systems fail to meet even minimum standards that any other test deployed in a public health laboratory would need to meet."[211]

Dr. George further testified as to inadequate interactions with states and localities whose personnel would be key actors in responding to an attack:

> "Late last year, the Department of Homeland Security announced a new initiative – Biodetection 21 or BD21 – to replace existing, inadequate BioWatch technology…The Department has not sought comprehensive input from relevant stakeholders…State, local, tribal, and territorial partners have been left almost entirely out of the loop. They are unsure if they can support the system, because no vision for it has been communicated to them, other federal partners, and Congress. These characteristics do not provide a good basis for success."[212]

Further, inadequate resources and funding for the public health sector have undercut the capacity to respond to adversarial biological threats. Dr. Rakeman testified:

> "[S]ignificant cuts in federal funding have hampered state and local readiness…[and] ha[ve] [led to] the significant reduction in the public health preparedness and response workforce in NYC. If there are no public health laboratory scientists, epidemiologists, environmental health specialists, emergency managers, and risk communication experts to build the local alarm system, and then hear the alarm and respond when it goes off, we cannot protect the health of the American public."[213]

The Government Accountability Office testified in March 2020, with a certain amount of understatement, that "challenges with planning to manage change; limited guidance and methods for analyzing capabilities; and lack of clarity about decision-making processes, roles, and responsibilities while adapting to a new enterprise-wide approach could limit the success of the [National Biodefense] Strategy's implementation."[214]

In light of these difficulties, Congress should require a multipart initiative with operational content to enhance biodefense against a potential adversarial attack. Congress will ultimately need to provide the required resources. To accomplish these ends:

208 E.g., George W. Bush, *Biodefense for the 21st Century* (Washington DC: White House), 2004, https://fas.org/irp/offdocs/nspd/hspd-10.html; Lisa O. Monaco, John P. Holdren, "A National Biosafety and Biosecurity System in the United States," October 29, 2015, https://obamawhitehouse.archives.gov/blog/2015/10/29/national-biosafety-and-biosecurity-system-united-states.

209 The White House, *National Biodefense Strategy*, 2018, 9-27, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf.

210 *Defending the Homeland from Bioterrorism: Are We Prepared?*, US House Committee on Homeland Security, 116th Cong. (2019) (statement of Asha M. George, DrPH, Executive Director, Bipartisan Commission on Biodefense), 3, https://docs.house.gov/meetings/HM/HM12/20191017/110097/HHRG-116-HM12-Wstate-GeorgeA-20191017.pdf.

211 *Defending the Homeland from Bioterrorism: Are We Prepared?*, US House Committee on Homeland Security, 116th Cong. (2019) (statement of Jennifer L. Rakeman, PhD, Assistant Commissioner and Laboratory Director New York City Department of Health and Mental Hygiene), 3, https://homeland.house.gov/imo/media/doc/Testimony-Rakeman.pdf.

212 *Defending the Homeland from Bioterrorism: Are We Prepared?*, US House Committee on Homeland Security, 116th Cong. (2019) (statement of Asha M. George, DrPH, Executive Director, Bipartisan Commission on Biodefense), 3, https://docs.house.gov/meetings/HM/HM12/20191017/110097/HHRG-116-HM12-Wstate-GeorgeA-20191017.pdf.

213 *Defending the Homeland from Bioterrorism: Are We Prepared?*, US House Committee on Homeland Security, 116th Cong. (2019) (statement of Jennifer L. Rakeman, PhD, Assistant Commissioner and Laboratory Director New York City Department of Health and Mental Hygiene), 3, https://homeland.house.gov/imo/media/doc/Testimony-Rakeman.pdf.

214 *National Biodefense Strategy, Opportunities and Challenges with Early Implementation*, US House Committee on Oversight and Reform, 116th Cong. (2020), (statement of Chris P. Currie, Director, Homeland Security and Justice, Government Accountability Office and Mary Denigan-Macauley, Director, Health Care, Government Accountability Office), 3, https://www.gao.gov/assets/710/705218.pdf.

First, Congress should review the status of biosurveillance programs and obtain a roadmap for the future. That will require expert testimony detailing the necessary resources and capabilities to implement the existing Strategy for Integrated Biosurveillance. As the testimony above noted, this strategy remains functionally insufficient in terms of actual implementation.[215] The National Security Commission on Artificial Intelligence cited above notes the role artificial intelligence could play to "detect pathogens with advanced sensing."[216]

Second, as part of its review of the Strategic National Stockpile, Congress should undertake to assure stockpile adequacy with respect to pathogens most likely to be utilized in an adversarial attack. The devastating deficiencies in the stockpile that have been exposed in the context of the coronavirus should not be allowed to continue. While the work to increase the stock of necessary supplies through the use of the Defense Production Act is ongoing, authorities should include many of the supplies needed for adversarial biological attacks. For such instances, there will be additional requirements such as "antitoxins…for several of the agents most likely to be used in a biological weapons attack."

Third, Congress should evaluate efforts by the Defense Advanced Research Projects Agency (DARPA) to determine whether that agency could productively undertake additional research relevant to biodefense. DARPA has a Biological Technologies Office, established in 2014, which has undertaken multiple programs.[217] The question is whether that office's programs should be expanded.

Fourth, Congress should evaluate whether the Department of Defense as a whole should give greater focus to homeland biodefense. This would include a functional review of the capabilities and activities of Northern Command, DARPA (per above), other DOD laboratories including Army Medical Research Institute of Infectious Disease [ARMRIID], and the National Guard. One particular element that needs analysis is the requirement for decontamination in the event that pathogens such as anthrax are used in an attack.

Fifth, Congress should require that the federal government undertake specific planning necessary to respond to an attack on one or several cities. Former Secretary of the Navy Richard Danzig had suggested "[d]evelop[ing] an immediately usable, detailed plan for coping with catastrophic attacks in one city that is especially at risk."[218] He recommended:

> "A useful innovation would…[be] a detailed collaboration with a single jurisdiction that is particularly at risk and, as a result of that risk, is particularly committed to planning and preparing in detail. Plans with that jurisdiction…should posit one or two particular risks from bioterrorism…Federal and local planners should then, in considerable detail, walk through the decisions that will need to be made in response to an attack (evacuation, operation of mass transit, means of decontamination, support of nonresident transients, and so forth). Federal-state-city agreement on these steps…can then be used as a basis for similar discussion and planning with [other] jurisdiction."[219]

The key point is to recommend action items that would translate to operational capabilities. The strategies set forth on paper for biodefense are perfectly reasonable. The actual capabilities are entirely insufficient.

"Congress should establish a Resilience Commission … that … looks at resilience … broadly."

C. Congress Should Establish a Resilience Commission

The actions needed to create a more resilient United States are substantial, and will affect both government and the private sector. To analyze and recommend certain necessary systemic changes, but especially to undertake continued factfinding as to the status of and requirements for effective resilience, Congress should establish a Resilience Commission. Such a commission would follow the same lines as the 9/11 Commission, the Cyberspace Solarium Commission, and the National Security Commission on Artificial Intelligence. Congressional engagement is critical to this issue, as the challenges posed by a pandemic or a comparable disruption raise political as well as substantive issues. A Resilience Commission should include

215 US Department of Homeland Security, *Strategy for Integrated Biosurveillance*, July 30, 2019, https://www.dhs.gov/sites/default/files/publications/cwmd_-_strategy_for_integrated_biosurveillance.pdf.

216 Matheny, Zetter, deBlanc-Knowles, and Garris, *The Role of AI Technology*, 10.

217 See Defense Advanced Research Projects Agency, Biological Technologies Office, https://www.darpa.mil/about-us/offices/bto?PP=1.

218 Danzig, *A Policymaker's Guide*, 23.

219 Ibid. pp.24-25.

knowledgeable participants from Congress, the administration, state and local governments, the private sector, and academia.

Congressional commissions have a long history in the United States. Generally, a Congressional commission will have the following characteristics:

> "Congressional advisory commissions are formal groups established to provide independent advice; to make recommendations for changes in public policy; to study or investigate a particular problem, issue, or event…While no legal definition exists for what constitutes a congressional commission,…a congressional commission is defined as a multimember independent entity that (1) is established by Congress, (2) exists temporarily, (3) serves in an advisory capacity, (4) is appointed in part or whole by Members of Congress, and (5) reports to Congress."[220]

The next administration and Congress itself will undoubtedly review multiple issues regarding resilience, in light of the pandemic. There are already multiple calls for a commission focused on lessons from the pandemic.[221] However, a broad-based Congressional commission that reviews the pandemic but looks at resilience more broadly, encompasses multiple expertise and perspectives, and operates on an ongoing basis including factfinding and future recommendations can have a more significant benefit to the country.

> "By establishing a commission, Congress can potentially provide a highly visible forum for important issues and assemble greater expertise than may be readily available within the legislature. Complex policy issues can be examined over a longer time period and in greater depth than may be practical for legislators. Finally, the nonpartisan or bipartisan character of most congressional commissions may make their findings and recommendations more politically acceptable, both in Congress and among the public."[222]

Congress has already established the COVID-19 Congressional Oversight Commission to review the implementation of the financial authorities given to the Department of the Treasury and the Federal Reserve to combat the economic effects of the virus.[223] However, the proposed Resilience Commission would have a much broader mandate, including but not limited to health and the pandemic—as the challenges of resilience are much broader.[224] As indicated, its composition should include participation from Congress, the executive branch, relevant independent agencies such as the Federal Reserve, state and local governments, elements of the private sector focused on key critical infrastructures most relevant to effective resilience, and academia. An outside commission with such expertise will have the necessary broad perspective both to understand the issues and to push for the type of changes required for operational and effective resilience.

The Resilience Commission would, as requested, undertake factfinding and construct recommendations for legislation to the Congress and comparable actionable recommendations to the administration so that the United States will be ready for the next pandemic or nationally consequential emergency. It would similarly act as a factfinding group to illuminate the landscape relevant to effective resilience including changes over time.

Perhaps as important as the specifics of its recommendations, the Resilience Commission could act in a leadership role ensuring that the country's desire to "get back to normal" does not impede the long-term actions necessary to prepare for and respond to the next pandemic or comparable national emergency, as well as longer-term resilience challenges. All too often in the face of traumatic events, there can be a "cycle of panic and neglect."[225] The challenges raised by pandemics, nationwide cyberattacks, or comparable events should not be met with panic but rather with a coordinated response that is the result of preparation, planning, and resolve. The nation deserves no less and the proposed Resilience Commission could be part of such a determined effective resilience effort.

220 Congressional Research Service, *Congressional Commissions: Overview and Considerations for Congress*, November 22, 2019, https://fas.org/sgp/crs/misc/R40076.pdf.

221 E.g., Editorial Board, "We Must Learn the Lessons of the Pandemic. A Bipartisan Commission Can Help With That," *Washington Post*, August 18, 2020, https://www.washingtonpost.com/opinions/we-must-learn-the-lessons-of-the-pandemic-a-bipartisan-commission-can-help-with-that/2020/08/18/ff5767dc-8a34-11ea-ac8a-fe9b8088e101_story.html.

222 Congressional Research Service, *Congressional Commissions: Overview and Considerations for Congress*, November 22, 2019, https://fas.org/sgp/crs/misc/R40076.pdf.

223 Congressional Research Service, *COVID-19 Congressional Oversight Commission*, April 2, 2020, https://crsreports.congress.gov/product/pdf/IN/IN11304.

224 A recent report called for a 'grand strategy of resilience" which, while including issues such as pandemics, climate change and cyber attacks, also discussed numerous other matters including economic inequality , trust in democracy, deepening alliances, the Internet as a utility, and many more. Ganesh Sitaraman, A Grand Strategy of Resilience, Foreign Affairs, September/October 2020, https://www.foreignaffairs.com/articles/united-states/2020-08-11/grand-strategy-resilience

225 "For too long, we have allowed a cycle of panic and neglect when it comes to pandemics: we ramp up efforts when there is a serious threat, then quickly forget about them when the threat subsides," *A World At Risk*, Global Preparedness Monitoring Board, September 2019, 6, https://apps.who.int/gpmb/assets/annual_report/GPMB_annualreport_2019.pdf.

V. CONCLUSION

Effective resilience should be a foundational objective of US national strategy and a fundamental driver of executive and Congressional action that necessarily will be in full partnership with the private sector. Effective resilience means the capacity to prepare for and withstand shocks of the magnitude of a major pandemic or equivalent, such as a major cyberattack with any resulting disruption significantly less than that caused by COVID-19. Effective resilience also needs to encompass preparations for longer-term challenges, including those posed by supply chain vulnerabilities as well as those from Chinese cyber espionage and state-driven economic practices. Establishing a Strategic Framework for Key Critical Infrastructure Resilience and a Strategic Framework for Health Sector and Biological Resilience will provide the structures necessary to meeting the challenges. The United States has successfully faced daunting challenges before, and by implementing the strategy recommended in this report the nation can likewise successfully meet the challenge of establishing effective resilience.

About the Author

Franklin D. Kramer is a Distinguished Fellow and on the board of the Atlantic Council. Mr. Kramer has been a senior political appointee in two administrations, including as Assistant Secretary of Defense for International Security Affairs. At the Department of Defense, Mr. Kramer was in charge of the formulation and implementation of international defense and political-military policy, with worldwide responsibilities including NATO and Europe, the Middle East, Asia, Africa and Latin America.

In the non-profit world, Mr. Kramer has been a Senior Fellow at CNA; chairman of the board of the World Affairs Council of Washington, DC; a Distinguished Research Fellow at the Center for Technology and National Security Policy of the National Defense University; and an adjunct professor at the Elliott School of International Affairs, George Washington University. Mr. Kramer's areas of focus include defense, both conventional and hybrid; NATO and Russia; cyber including resilience and international cyber issues; irregular conflict and counterinsurgency; innovation and national security; and China including managing competition, military power, and China-Taiwan-US relations.

Mr. Kramer has written extensively; in addition to the current report on "Effective Resilience and National Strategy: Lessons from the Pandemic and Requirements for Key Critical Infrastructures," his publications include "Managed Competition: Meeting China's Challenge in a Multi-vector World"; on NATO, "NATO Priorities After the Brussels Summit" and "Meeting the Russian Hybrid Challenge"; on cyber "Cybersecurity: Changing the Model," "Cyber and Deterrence: The Military-Civil Nexus in High-End Conflict," and "Cyber, Extended Deterrence, and NATO"; on innovation, "Innovation, Leadership, and National Security"; and on counterinsurgency, he was the principal editor, and co-author of the policy chapter, of the book "Civil Power in Irregular Conflict" and "Irregular Conflict, The Department of Defense and International Security Reform."

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

CHAIRMAN EMERITUS
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stéphane Abrial
Odeh Aburdene
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
Matthew C. Bernstein
*Rafic A. Bizri
Linden Blue
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Robert S. Gelbard
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
*Amir A. Handjani
Katie Harbath
John D. Harris, II
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
Stephen R. Kappes
*Maria Pica Karp
Andre Kelleners
Astri Kimball Van Dyke
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Neil Masterson
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Hilda Ochoa-Brillembourg
Ahmet M. Ören
Sally A. Painter
*Ana I. Palacio
*Kostas Pantazopoulos
Carlos Pascual
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Rajiv Shah
Stephen Shapiro
Wendy Sherman
Kris Singh
Christopher Smith
James G. Stavridis
Richard J.A. Steele
Mary Streett
Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
George P. Shultz
Horst Teltschik
John W. Warner
William H. Webster

**Executive Committee Members*
List as of June 30, 2020

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org