Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence

White Paper Series on Pandemic Response and Preparedness, No. 2

NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE

Disclaimer: This white paper only reflects the views of the contributing Commissioners and staff and does not reflect official views or recommendations of the full Commission.

Letter from the Executive Director

As we note in our interim report to the Congress from November 2019, the development of artificial intelligence (AI) will shape the future of power. The nation with the most resilient and productive economic base will be best positioned to seize the mantle of world leadership. That base increasingly depends on the strength of the innovation economy, which in turn will depend on AI.[1]

The global crisis initiated by the COVID-19 pandemic poses a unique threat to the national security and economic competitiveness of the United States. The ongoing financial turmoil has also highlighted existing gaps and deficiencies in U.S. and allied supply chains, as well as their national security implications. During this crisis, the United States Government must work to protect the integrity, resilience, and long-term viability of both of these systems. Those efforts should include using AI to help safely reopen the economy, preventing foreign exploitation of key elements of the U.S. technology base, and by identifying and correcting vulnerabilities in supply chains that are critical to national security.

Given the magnitude of the crisis, and the national security implications, I believe the National Security Commission on Artificial Intelligence (NSCAI) has a responsibility to offer recommendations to protect America's economic security and leave the nation in a stronger position after the crisis.

We have initiated temporary special projects to issue white papers that address AI-related aspects of pandemic response and implications of the crisis for America's security and strategic competitiveness. Each paper is a collaboration of participating Commissioners and select staff, and only reflects the views of the Commissioners and staff who have contributed to the special project. It does not reflect official action, deliberation, or decision by the NSCAI, all 15 Commissioners, a majority of Commissioners, or any Commissioner who was not part of the special project that produced the paper. These special projects are separate and distinct from the Commission's current lines of effort.

Four NSCAI Commissioners issued the first white paper, "Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID-19," analyzing how computing applications can supplement the United States' manual

---

[1] *Interim Report*, NSCAI (Nov. 5, 2019), https://www.nscai.gov/reports.

contact tracing efforts and recommending privacy and ethics considerations in developing and fielding these applications.

The second white paper, "Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in AI," offers recommendations for using AI to mitigate the economic impact of COVID-19, and for protecting AI and other emerging technologies as strategic assets and sources of U.S. and allied economic strength.

As always, we welcome your comments and feedback submitted via congress@nscai.gov.

Ylli Bajraktari
Executive Director

Mitigating Economic Impacts of the COVID-19 Pandemic and Preserving U.S. Strategic Competitiveness in Artificial Intelligence[2]

National Security Commission on Artificial Intelligence Commissioners Chris Darby, Gilman Louie, and Dr. Jason Matheny[3]

The COVID-19 pandemic presents significant challenges for the United States' economy and by extension its strategic competitiveness. The duration of the economic downturn and its effects on the technology sector will determine whether the United States preserves its advantages in artificial intelligence (AI) and other emerging technologies critical to national security.

Consistent with the mandate of the National Security Commission on Artificial Intelligence (NSCAI)[4], this White Paper offers several steps policymakers could take to utilize and protect U.S. capabilities in AI and associated technologies during the current crisis and beyond. AI presents opportunities to help safely reopen and grow the U.S. economy while minimizing the risk of future outbreaks of the virus, but the

---

[2] This white paper reflects the views of the commissioners and staff who have participated in this special project on privacy and ethics recommendations for computing applications developed to mitigate COVID-19. It does not reflect official action, deliberation, or decision by the NSCAI, all 15 commissioners, a majority of commissioners, or any commissioner who was not part of this special project.

[3] Commission staff who contributed to this special project white paper include Kevin McGinnis and Chris McGuire.

[4] The U.S. Congress established the Commission, mandating that it "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." The John S. McCain National Defense Authorization Act for Fiscal Year 2019, Sec. 1051, Pub. L. 115-232, 132 Stat. 1636, 1962-65 (2018), as amended by the National Defense Authorization Act for Fiscal Year 2020, Sec. 1735, Pub. L. 116-92 (2019).

AI ecosystem itself is one of the most critical sectors in need of assistance and protection from foreign competitors as it weathers the brutal economic crisis. At the same time, policymakers must be circumspect about AI's ability to solve all of the problems created by the pandemic, especially in areas where there is not enough data to fuel machine learning applications.

Although many of the largest technology companies are thriving, innovative startups and other small firms working on technologies with national security implications are vulnerable during this unprecedented economic crisis. Such firms will need help sustaining their technological and human capital if the United States wants its diverse technology ecosystem to thrive. Additionally, strategic competitors covet tech companies' know-how and intellectual property, and have a track record of transferring these assets for their benefit via licit and illicit means. If firms developing critical technologies face dire economic conditions, they could be particularly vulnerable to purchase by a strategic competitor. In late March, Undersecretary of Defense Ellen Lord underscored this concern, warning that, "it is critically important that we understand that during this crisis, the [defense-industrial base] is vulnerable to adversarial capital, so we need to ensure that companies can stay in business without losing their technology."[5]

The Tech Competition Continues: The strategic competition between the United States and China, fueled by technology developments, has not slowed down during the COVID-19 crisis; rather, it may be accelerating. The pandemic may substantially alter the economic playing field between the United States and China, presenting new risks and opportunities for both sides. Although China suffered more economic distress than the United States in Quarter (Q) 1 2020, with its economy contracting by 6.8 percent on an annualized basis[6] compared to 4.8 percent for the United States,[7] economists project China's growth will be largely flat in Q2,[8] whereas the Congressional Budget Office estimates that the U.S. gross domestic product will contract by approximately 40 percent

---

[5] Aaron Mehta & Valerie Insinna, *Amid Pandemic, Pentagon Urges 'Hyper-vigilance' Against Foreign Investment*, DefenseNews (Mar. 25, 2019), https://www.defensenews.com/coronavirus/2020/03/25/amid-pandemic-pentagon-urges-hyper-vigilance-against-foreign-investment/.

[6] Vivek Mishra, *China on Slow Road to Recovery, but Recession Risk is High: Reuters Poll*, Reuters (Apr. 22, 2020), https://www.reuters.com/article/us-china-economy-poll/china-on-slow-road-to-recovery-but-recession-risk-is-high-reuters-poll-idUSKCN22502B [hereinafter Mishra, China on Slow Road to Recovery].

[7] *Gross Domestic Product*, Bureau of Economic Analysis (last visited May 13, 2020), https://www.bea.gov/data/gdp/gross-domestic-product.

[8] Mishra, China on Slow Road to Recovery.

on an annualized basis over the same period.[9] These projections must be taken with a grain of salt given the fast-moving and dynamic nature of the crisis, and China could face significant economic headwinds if many businesses decide to move their manufacturing operations out of China. However, should a significant disparity in growth occur, it would have profound national security implications, including for the United States' ability to retain leadership in key emerging technologies such as artificial intelligence.

Additionally, the Chinese government's management of its economy during the pandemic makes clear that it will not scale down its high-tech ambitions in the face of the public health crisis. Beijing granted special waivers to key microelectronics firms to continue full production and ignore quarantine guidelines while entire cities were shut down, including to Yangtze Memory Technologies Co.'s plant in Wuhan.[10] Furthermore, the Chinese government's actions to nationalize its entire medical supply industry and restrict the export of medical personal protective equipment (PPE), including by American companies operating in China such as 3M, highlight critical existing U.S. supply chain vulnerabilities.[11]

Faced with this challenging reality, the United States must determine ways to utilize AI to reset the economic playing field, mitigate vulnerabilities exposed by this crisis, and work to prevent competitors led by China from exploiting the current economic disruption to provide them long-term advantages in key technologies. While these recommendations focus on AI and associated technologies, it is important to note that the intersection of national security and other emerging technologies, such as biotechnology, also require policymaker attention during this crisis.

The following recommendations provide a roadmap of steps the United States should take to ensure it emerges from this crisis in a stronger position, and prevent adversaries from taking advantage of the U.S. technology sector as the country gains control over the pandemic and restores the economy to a growth trajectory.

---

[9] Phill Swagel, CBO's Current Projections of Output, Employment, and Interest Rates and a Preliminary Look at Federal Deficits for 2020 and 2021, Congressional Budget Office (Apr. 24, 2020), https://www.cbo.gov/publication/56335.

[10] Cheng Ting-Fang & Lauly Li, *How China's Chip Industry Defied the Coronavirus Lockdown*, Nikkei Asian Review (Mar. 18, 2020), https://asia.nikkei.com/Spotlight/Cover-Story/How-China-s-chip-industry-defied-the-coronavirus-lockdown.

[11] Keith Bradsher & Liz Alderman, *The World Needs Masks. China Makes Them, but Has Been Hoarding Them*, New York Times (Apr. 2, 2020), https://www.nytimes.com/2020/03/13/business/masks-china-coronavirus.html.

These recommendations fall into five categories for using AI to mitigate the economic impact of COVID-19 and protecting AI and other emerging technologies as strategic assets and sources of U.S. and allied economic strength. Specific recommendations in this memo focus on using AI to: 1) Inform efforts to safely **reopen** the U.S. economy; 2) **Assess** the strengths and vulnerabilities of the national security supply chain; 3) **Preserve** small- and medium-size technology firms critical to national security in order to protect U.S. AI advantages; 4) **Screen** for adversarial predatory investments; and 5) **Return** key supply chains by expanding U.S. and allied production of critical goods.

Recommendation 1: Reopen - Utilize AI to Inform Reopening the Economy

As the United States begins to move toward reopening elements of its economy, a data driven and analytical approach can minimize the risk of future outbreaks of COVID-19. This approach will both increase public confidence in the safety of engaging in commercial activity, which will expedite recovery efforts, and ideally prevent the growth of future outbreaks which would lead to a return to strict shutdowns. As a precondition for this effort and in the absence of a vaccine or widespread, effective treatment, communities will require accurate underlying data about the local spread of COVID-19 so policymakers and citizens can fully understand risk factors. Comprehensive testing combined with effective contact tracing is the most thorough way to measure the total number of infections in a given population,[12] although sophisticated disease modeling and forecasting techniques may be able to quickly and accurately assess disease prevalence by synthesizing disparate data streams—again, assuming sufficiently accessible and accurate underlying data.[13] For example, studies suggest hospital traffic extracted from satellite imagery of hospital parking lots is useful as an estimator of disease activity, specifically influenza-like illnesses.[14] Fundamentally,

---

[12] Four NSCAI Commissioners issued a white paper with a detailed analysis of how computing applications can supplement the United States' manual contact tracing efforts and recommended privacy and ethics considerations in developing and fielding these applications. See *Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID-19*, NSCAI (May 6, 2020), https://www.nscai.gov/reports.

[13] The Commission plans to potentially discuss this topic in greater detail in a future white paper in this series, which may offer additional recommendations on this topic.

[14] Elaine Nsoesie, et al., Monitoring Disease Trends using Hospital Traffic Data from High Resolution Satellite Imagery: A Feasibility Study, Scientific Reports (Mar. 13, 2015), https://www.nature.com/articles/srep09112.

regional economic reopenings should be associated with access to accurate data about the local spread of COVID-19.

Once policymakers have access to accurate local COVID-19 data, tailored AI-enabled platforms can analyze data regarding both the state of the economy and spread of the virus to model projected risk and benefit from specific policy actions. Such tools, once properly validated and using accurate underlying data, could assist policymakers at all levels in projecting the economic and health impacts of releasing shutdowns, reopening schools, or opening specific types of businesses in individual communities. This would also allow for more granular and tailored policy responses, which would maximize economic benefit while minimizing risk, and also permit policymakers to monitor outcomes over time. Should such a granular and data-driven approach prove safer than across-the-board openings, it would likely also lead to a faster economic rebound, as it would enhance confidence in public safety and increase individuals' willingness to leave their homes and engage in commerce.[15]

In the near-term, every governor should commission a data-driven support tool —designed with input from economists, medical professionals, and machine learning experts—which integrates both economic and public health data to inform their state's reopening process. Pennsylvania has led the way in this effort, as Governor Tom Wolf recently announced a partnership with Carnegie Mellon University to develop exactly such a tool, which should serve as a model for other states.[16] Additionally, the University of Virginia's Biocomplexity Institute and Initiative is developing a similar tool, which it plans to make widely available to policymakers throughout the country.[17] These two models should serve as pilot programs for other states' efforts. Pennsylvania and potentially Virginia should work to validate the models' methods and assumptions to enhance their accuracy, and assist the design of similar models being developed for other states.

---

[15] Currently, many states that have begun lifting shutdown measures are seeing very slow rebounds, which can be attributed to a continued reluctance to leave the house and engage in behavior deemed to be risky. See David Harrison & Justin Baer, *As States Begin to Reopen, Many Stay Home—Keeping Economic Rebound Elusive*, Wall Street Journal (May 2, 2020), https://www.wsj.com/articles/as-states-begin-to-reopen-many-stay-homekeeping-economic-rebound-elusive-11588411801?mod=hp_lead_pos1.

[16] *Process to Reopen Pennsylvania*, Governor Tom Wolf (May 12, 2020), https://www.governor.pa.gov/process-to-reopen-pennsylvania/. For additional details on the dashboard, see also *CMU Dashboard Will Help Inform State Decision-Makers During Pandemic*, Carnegie Mellon University (Apr. 22, 2020), https://www.cmu.edu/news/stories/archives/2020/april/dashboard-will-help-inform-state-decision-makers.html.

[17] Jared Council, *AI Platform Aims to Help Policy Makers Calibrate Virus Response*, Wall Street Journal (Mar. 24, 2020), https://www.wsj.com/articles/ai-platform-aims-to-help-policy-makers-calibrate-virus-response-11585042201.

In the longer-term, the Federal Government should establish the data availability, infrastructure, and analytical capacity necessary to conduct such analysis across the country, so that it has the ability to partner with states on locally-calibrated steps to best balance economic and public health risks. While AI has the potential to assist with the current crisis, it also faces structural limitations due to the current lack of available, accurate, and relevant data. For instance, most hospital records still exist only on paper and have not been digitized, and are therefore unable to feed AI models.[18] As a result, there will be challenges that cannot be addressed by AI in this crisis, but which AI could help solve in future pandemic scenarios. It is incumbent on the Federal Government to ensure the proper disease surveillance and data standards are in place in the future so that accurate and up-to-date data about disease spread is readily available and able to improve AI-enabled decision making tools for policymakers. By applying the right mix of talent, vision, and funding, the nation can be better prepared to face the next pandemic with data-driven, AI enabled decision-making.

Recommendation 2: Assess - Understand the National Security Supply Chain

Companies across all sectors are already re-examining and re-thinking their supply chains in response to the pandemic.[19] Tracing every item back to its source is difficult and costly due to the depth, scope, and fluidity of global supply chains. As COVID-19 highlights, some strategic sectors deserve that level of scrutiny, especially advanced technology, healthcare, defense, and related industries.[20] For example, suppliers in China issued over 3,000 force majeure certificates for contract cancellations for exports

---

[18] Darius Tahir, *Virus Hunters Rely on Faxes, Paper Records as More States Reopen*, Politico (May 10, 2020), https://www.politico.com/news/2020/05/10/coronavirus-health-records-245483.

[19] Andrew Edgecliffe-Johnson, *US Supply Chains and Ports Under Strain from Coronavirus*, Financial Times (Mar. 2, 2020), https://www.ft.com/content/5b5b8990-5a98-11ea-a528-dd0f971febbc.

[20] Aaron Friedberg & Charles Boustany Jr., *Partial Disengagement: A New US Strategy for Economic Competition with China*, The Washington Quarterly (Mar. 19, 2020), https://cpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2020/03/FriedbergBoustany_43-1.pdf [hereinafter Friedberg, Partial Disengagement]. For example, a recent assessment of 3M and Rockwell Collins--two of the Defense Logistics Agencies largest suppliers--showed they relied on more than 1200 sub-vendors, many of which are tied to China, Russia, and other risky nations. See Michael Kidd, *Social Network Analysis of DoD Supply Chain Vulnerabilities*, Small Wars Journal (last visited May 14, 2020), https://smallwarsjournal.com/jrnl/art/social-network-analysis-dod-supply-chain-vulnerabilities [hereinafter Kidd, Social Network Analysis].

worth more than $38 billion due to COVID-19 in February alone.[21] Closer to home in North America, factory shutdowns in Mexico have disrupted U.S. supply chains for PPE, aerospace manufacturing, and other unanticipated sectors.[22]

The United States Government has known about problems with its supply chain for at least 30 years. The Government Accountability Office (GAO) listed the Department of Defense's (DoD) supply chain management as one of its government-wide high risk areas from 1990 to 2019, only removing it last year after DoD finally demonstrated "sufficient progress."[23] But GAO's past reviews focused on inventory management rather than vulnerabilities to critical and emerging technology supply chains. To its credit, the Federal Government has undertaken a multi-pronged, concerted effort to identify and address national security supply chain vulnerabilities since 2017 under Executive Order 13806 and in response to Section 1071 of the National Defense Authorization Act for Fiscal Year (FY) 2017, well before the current crisis began.[24] Those efforts must now go deeper and faster.

To start, **the United States Government should expand its capacity to analyze relevant commercial and technical information about supply chains using machine learning.**[25] Working with the private sector, it must develop and deploy new tools and analytic techniques to identify high risk nodes in its complex and rapidly evolving supply chains.[26] This is already an area of promising investment in the

---

[21] Sun Yu & Xinning Liu, *China Issues Record Number of Force Majeure Certificates*, Financial Times (Feb. 27, 2020), https://www.ft.com/content/bca84ad8-5860-11ea-a528-dd0f971febbc.

[22] Sabrina Rodriguez, *Sweeping Mexican Factory Shutdown Strains U.S. Production of Critical Supplies*, Politico (Apr. 27, 2020), https://www.politico.com/news/2020/04/27/mexico-american-production-coronavirus-212971.

[23] U.S. Gov't Accountability Office, GAO-19-157SP, High Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas (2019), https://www.gao.gov/products/GAO-19-157sp.

[24] Executive Order 13806, *Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, The White House (July 21, 2017), https://www.whitehouse.gov/presidential-actions/presidential-executive-order-assessing-strengthening-manufacturing-defense-industrial-base-supply-chain-resiliency-united-states/; National Defense Authorization Act for Fiscal Year 2017, Sec. 1071, Pub. L. 114-328, 130 Stat. 2000 (2016).

[25] "An [AI-enabled] enterprise assessment of potential supply chain risks, to include likelihood of occurrence and severity, should . . . [show] . . . overall supply chain risk-impact factor calculation for all networked vendors." See Kidd, Social Network Analysis.

[26] Friedberg, Partial Disengagement.

commercial sector and a recent survey reported 32 percent of venture capitalists planned to increase their investments in the logistics sector as a result of COVID-19.[27]

Yet even with the best tools, an analysis of the supply chain is only as good as the data available. That data that is not easily accessible, in part because it is not transparently reported. Recent improvements in supply chain risk management prior to COVID-19 focused on identifying and reducing cybersecurity vulnerabilities among contractors and subcontractors.[28] Yet the current crisis demonstrates that the United States Government needs deeper awareness of the vendors and sub-vendors it is relying upon around the world in a range of product categories, not simply cybersecurity.

To expand national security supply chain data and visibility, the United States Government should revise the Defense Federal Acquisition Regulation Supplement to require additional disclosure and reporting requirements on the location of manufacturing centers for firms supplying critical systems and subsystems for the U.S. military. DoD has existing information requirements for certain items and systems related to the defense supply chain, including procedures for making determinations and notifications of a "significant supply chain risk to a covered system."[29] However, additional information would enable the United States Government and other firms to better identify vendors and sub-vendors in nations that pose risks to the United States. When a company is unable to identify the locations of its suppliers' manufacturing nodes, it could be an indicator that they require further scrutiny or should not be relied upon to supply the United States Government with strategically important products.[30] Paired with an oversight mechanism, this increase in transparency would empower officials to weigh the risks before agreeing to a particular contract and also respond more effectively to unexpected disruptions such as COVID-19.

---

[27] *500 Startups Survey Results: The Impact of COVID-19 on the Early Stage Investment Climate*, 500 Startups (2020), https://drive.google.com/file/d/1DHDlFWxRL75rpy_A7tL1RrbhXfbYh-dk/view [hereinafter 500 Startups Survey Results].

[28] Brian P. Cruz et al., *Department of Defense Makes Supply Chain Cybersecurity Provision Permanent*, Pillsbury (Oct. 10, 2018), https://www.pillsburylaw.com/en/news-and-insights/dod-makes-supply-chain-cybersecurity-provision-permanent.html.

[29] Existing requirements can be found here, *Subpart 239.73 - Requirements for Information Relating to Supply Chain Risk*, DoD Defense Federal Acquisition Regulation Supplement (Feb. 15, 2019), https://www.acq.osd.mil/dpap/dars/dfars/html/current/239_73.htm.

[30] Tara Beeny, *Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology*, Interos (Apr. 2018), https://docs.house.gov/meetings/IF/IF16/20180516/108301/HHRG-115-IF16-20180516-SD105-U105.pdf.

Finally, beyond better tools and data, it is clear that supply chains are a long-term challenge requiring dedicated and sustained focus within the United States Government. **Legislation drafted last year proposed creating a whole-of-government National Supply Chain Intelligence Center.**[31] **This is needed now more than ever.**

Recommendation 3: Preserve - Provide Government Support to Small and Medium-Sized Technology Firms Critical to National Security

The decrease in availability of capital to critical small- and medium-sized U.S. firms as a result of the economic slowdown, particularly in the technology industry, poses acute national security risks to the United States.[32] A recent survey of small- and medium-sized U.S. businesses in the defense sector reported that 60 percent of such firms expect to have long-term financial and cash-flow issues as a result of the crisis, with defense technology firms reporting more significant negative anticipated impacts than any other sector.[33] Such firms are key to both overall U.S. leadership in emerging technologies and the Federal Government's ability to leverage the technology sector for national security benefit. For instance, defense leaders have expressed concerns that a slowdown in commercial investment in space companies and satellite design—where only 20 percent of the research and development (R&D) investment comes from the United States Government and 80 percent from commercial investors—could stifle innovation for the duration of the crisis.[34] DoD's recent announcement that it will make $3 billion in new progress payments to increase cash flow among defense

---

[31] *Crapo, Warner Legislation Would Secure U.S. Supply Chains against Foreign Exploitation*, Sen. Mike Crapo (Jul. 30, 2019), https://www.crapo.senate.gov/media/newsreleases/crapo-warner-legislation-would-secure-us-supply-chains-against-foreign-exploitation-; Chris Nissen et al., *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*, MITRE (Aug. 2018), https://www.dni.gov/files/NCSC/documents/supplychain/20190327-Deliver-uncompromised.pdf; *AI and IoT Legislative Developments: Third Quarter 2019*, Covington (Oct. 21, 2019), https://www.cov.com/-/media/files/corporate/publications/2019/10/ai_and_iot_legislative_developments_third_quarter_2019.pdf.

[32] In April 2020, a survey of venture capital firms found that 68 percent anticipated that COVID-19 would "have a negative or somewhat negative impact on early-stage investment activity in 2020." See 500 Startups Survey Results. Additionally, a recent report from the National Venture Capital Association stated that "existing capital reserves by venture capital (VC) investment funds will not be nearly enough to sustain operations in the startup ecosystem." Maryam Haque & Justin Field, *Startup Ecosystem Faces Capital Crunch over Coming Months*, National Venture Capital Association (Apr. 27, 2020), https://nvca.org/wp-content/uploads/2020/04/Startup-Ecosystem-Faces-Capital-Crunch-over-Coming-Months-4.pdf.

[33] Corbin Evans & Camilla Shanley, NDIA COVID-19 Small-Business Impacts Survey Summary, NDIA (Apr. 23, 2020), https://www.ndia.org/-/media/sites/ndia/policy/documents/covid-19-small-business-impacts-survey-summary.ashx.

[34] Sandra Erwin, *Venture Capital Slowdown a Concern for Military Space Programs, Analysts Warn*, SpaceNews (Apr. 27, 2020), https://spacenews.com/venture-capital-slowdown-a-concern-for-military-space-programs-analysts-warn/.

contractors and specifically provide support to the space industry is a good step, but additional targeted actions are necessary.[35]

In order to preserve U.S. competitiveness, **the United States must ensure that small- and medium-sized U.S. firms in key emerging technologies, including private equity and venture capital-backed firms, have access to capital for the duration of the economic slowdown. In addition, individual services and agencies should establish rapid technology procurement funds geared at small and medium sized emerging tech businesses,** which would contract firms to quickly solve high-priority technology problems agencies are currently facing. Such programs will both inject needed capital into critical small- and medium-sized technology firms, and ensure the United States Government sees immediate benefit. The U.S. Air Force has been a leader in this area already, awarding nearly $1 billion to 599 small business contracts at the beginning of the outbreak, and also dedicating $350 million to AFWERX to battle the virus.[36] Other services and agencies should stand up similar efforts, and the United States Government should expand existing efforts focused on the space industry to also include AI firms.

One area to fund should be the Defense Innovation Unit's (DIU) National Security Innovation Capital Program. In Fiscal Year 2019, the Congress authorized $75 million for the program's activities. To date, however, the Congress has not appropriated any funding. DIU's efforts in this area should be informed by an advisory board of public and private leaders who can help guide NSIC and translate priority problems to the commercial sector.[37] Current DoD efforts focused on the space sector, which are being informed by a rapidly assembled

---

[35] Michael Sheetz, *The US Government is Helping Get Cash to Private Space Companies, Replacing Frozen Venture Capital*, CNBC (Apr. 24, 2020), https://www.cnbc.com/2020/04/24/us-government-getting-cash-to-private-space-companies-replacing-venture-capital.html.

[36] Scott Maucione, *Air Force Says Space Industry Needs Stimulus as Economy Fails*, Federal News Network (Apr. 16, 2020), https://federalnewsnetwork.com/air-force/2020/04/air-force-says-space-industry-needs-stimulus-as-economy-fails/; see also *Covid-19 National Response Team*, AFWERX (last visited May 13, 2020), https://www.afwerx.af.mil/coronavirus.html.

[37] DIU's NSIC is focused on dual-use hardware startups. Its mission is to leverage DoD laboratories, national laboratories, academic laboratories, hardware-focused incubators, and venture capital firms to identify relevant startups that are seeking financing in the form of grants, loans, or equity. Specifically, this program is focused on early-stage hardware companies with difficulty raising sufficient capital from U.S. investors, presenting long-term supply chain risks for the U.S. economy. The areas NSIC has identified as its initial focus include quantum devices, rare earth processing technologies, small unmanned aerial systems, space systems components, and high-density batteries. See *About*, DIU (last visited May 14, 2020), https://www.diu.mil/about; *Exhibit R-2 RDT&E Budget Item Justification*, DoD at 1-2 (Feb. 2019), https://www.dacis.com/budget/budget_pdf/FY20/RDTE/D/0604341D8Z_99.pdf.

panel of private sector leaders who are offering advice on pandemic-related industrial base programs, can serve as a model for DIU and other similar efforts.[38]

Recommendation 4: Screen - Enhance Foreign Investment Screening

In addition to taking actions to promote innovation domestically during the crisis and helping innovative firms access alternative trusted sources of capital (see Recommendation 3), the United States must also prevent competitor nations from exploiting the current lack of liquidity in order to acquire sensitive technologies or intellectual property. While the recent Committee on Foreign Investment in the United States (CFIUS) reform legislation, the Foreign Investment Risk Review Modernization Act (FIRRMA), made important changes to the investment review process and expanded CFIUS to cover key "emerging and foundational technologies,"[39] delays in implementation of critical regulations has slowed CFIUS' expansion. In recognition of the threat that adversarial capital poses to the defense industrial base, the Department of Defense started the Trusted Capital Marketplace Program in the Fall of 2019 to connect sellers of emerging defense technologies with trusted buyers.[40]

Despite recent attention to the problem, the current economic environment poses acute risks and challenges and U.S. allies and partners are also taking notice of this threat. In late March 2020, Australia mandated that all new foreign investments be approved by its Foreign Investment Review Board, regardless of value.[41] India implemented a similar restriction for countries with which India shares a border, a move widely interpreted to be "aimed at China."[42] Spain and Italy have tightened their investment review thresholds and expanded reviewable sectors, and the European Union (EU) issued new guidance urging member states to make use of all available tools to prevent foreign

---

[38] Tom Roeder, *Pentagon Focused on Keeping Small Innovative Space Firms Healthy Through Coronavirus Downturn*, The Gazette (Apr. 26, 2020), https://gazette.com/military/pentagon-focused-on-keeping-small-innovative-space-firms-healthy-through-coronavirus-downturn/article_9cbee050-866f-11ea-97c0-e7925a3aa1dc.html.

[39] See Pub. L. 115-232, 132 STAT. 1636, 2173-2240 (Division a, Title XVII - Review of Foreign Investment and Export Controls).

[40] Jon Harper, Just In: Pentagon To Kick Off First 'Trusted Capital Marketplace' Event, National Defense Magazine (October 18, 2019), https://www.nationaldefensemagazine.org/articles/2019/10/18/pentagon-about-to-kick-off-first-trusted-capital-marketplace-event

[41] Fumi Matsumoto, *Australia Tightens Foreign Investment Rules after Market Tumble*, Nikkei Asian Review (Apr. 14, 2020), https://asia.nikkei.com/Politics/International-relations/Australia-tightens-foreign-investment-rules-after-market-tumble2.

[42] Aditya Kalra & Aftab Ahmed, *India Toughens Rules on Investments from Neighbours, Seen Aimed at China*, Reuters (Apr. 18, 2020), https://www.reuters.com/article/us-health-coronavirus-india-investments/india-toughens-rules-on-investments-from-neighbours-seen-aimed-at-china-idUSKBN2200LQ.

investment from non-EU countries which undermine Europe's security, and establish a mechanism to do so if one is not available.[43] EU competition chief Margrethe Vestager has urged EU governments to buy stakes in key companies to prevent foreign takeovers, if necessary.[44]

The United States must continue approving permissible CFIUS requests rapidly so firms have access to alternative sources of funding while also enhancing its vigilance regarding potential illicit technology transfers for the duration of the crisis, particularly in critical technology sectors. Enhancing investment screening alone cannot solve the relevant economic challenges associated with the crisis; until sufficient liquidity returns to U.S. capital markets, the U.S. technology ecosystem, particularly among small- and medium-sized firms, will continue to face significant distress. In addition to the critical steps outlined in Recommendation 3 which seek to preserve such firms' access to capital, the United States can also take the following steps to ensure that U.S. strategic competitors are not able to exploit the economic crisis for their benefit.

First, the United States should closely monitor foreign investment activity in the sectors the Department of Commerce identified as potential "emerging technologies that are essential to the national security of the United States" in 2018.[45] Although Commerce has yet to formally define "emerging and foundational technologies," the Department of Commerce list offers a comprehensive register of sectors that the United States should closely monitor throughout the current crisis. Should the United States see a spike in investment activity from China or other strategic competitors across these sectors, it should consider additional measures, to include mandatory CFIUS filings for all investments from countries currently on the

---

[43] Giampaolo Salsi et al., *COVID-19: Stricter Rules on FDI Screening in Italy, in the Wake of the Health and Sanitary Emergency*, JD Supra (Apr. 15, 2020), https://www.jdsupra.com/legalnews/covid-19-stricter-rules-on-fdi-31203/.

[44] Javier Espinoza, *Vestager Urges Stakebuilding to Block Chinese Takeovers*, Financial Times (Apr. 12, 2020), https://www.ft.com/content/e14f24c7-e47a-4c22-8cf3-f629da62b0a7.

[45] This list, includes technology related to: biotechnology; artificial intelligence and machine learning; position, navigation, and timing; microprocessors; advanced computing; data analytics; quantum information and sensing; advanced logistics; additive manufacturing; robotics; brain-computer interfaces; hypersonics; advanced materials; and advanced surveillance capabilities. See Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201 (Nov. 19, 2018), https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

International Traffic in Arms Regulations presumptive denial list for defense articles and defense services.[46]

Second, the Department of Commerce must finalize its list of "emerging and foundational technologies" as required under the Export Control Reform Act (ECRA) of 2018 as soon as possible. FIRRMA mandates that any technologies identified through this process will immediately become subject to a mandatory CFIUS filing, but absent a formal decision by Commerce any filings in these fields are voluntary unless the transaction in question is covered by separate regulations.[47] While the Department of the Treasury smartly codified the "critical technology pilot program" into the final FIRRMA regulations that took effect in February 2020 in order to require CFIUS filings for certain key industries such as space vehicles and semiconductors, this list does not include AI or many other critical emerging technologies.[48] Finalizing this list as required by ECRA is a necessary and long-overdue step to strengthen the investment screening regime, which is only underscored by the current crisis.

Finally, the United States must continue to closely coordinate its approach on investment screening with its allies and partners, including quickly sharing information about trends in investment flows in emerging technologies throughout the crisis. The crisis affords an important opportunity to highlight the threats global emerging technology industries face from predatory foreign investments, particularly as U.S. allies and partners remain in a vulnerable economic state. The Departments of State and Treasury have jointly helped build out allied investment screening capacity in recent years, but this effort must now take on increased urgency. State and Treasury should diligently share data about recent patterns in investment

---

[46] Part 126.1 of Title 22 of the U.S. Code of Federal Regulations lists the countries for which the United States currently has a policy of denial for exports of defense articles and defense services. This list contains the following countries: Belarus, Burma, China, Cuba, Iran, North Korea, Syria, Venezuela. See 22 CFR § 126.1 (d)(1), https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=70e390c181ea17f847fa696c47e3140a&mc=true&r=PART&n=pt22.1.126#se22.1.126_11.

[47] FIRRMA mandates that any transactions involving technologies that Commerce identifies as "emerging and foundational technologies" under ECRA also be subject to CFIUS review See Pub. L. 115-232, 132 STAT. 1636, 2173-2240 (Division A, Title XVII - Review of Foreign Investment and Export Controls); see also *The Emerging List of 'Emerging and Foundational Technologies'*, Jones Day (Nov. 2018), https://www.jonesday.com/en/insights/2018/11/the-emerging-list-of-emerging-and-foundational-tec. Commerce issued a proposed list of such technologies in November 2018, but progress on finalizing it has stalled. See Alexandra Alper, *Lawmakers Urge U.S. Government to Tighten Export Controls to China on Security Fears*, Reuters (Nov. 18, 2019), https://www.reuters.com/article/us-china-usa-exportcontrols-idUSKBN1XS2BI.

[48] Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112 (Jan. 17, 2020), https://home.treasury.gov/system/files/206/Part-800-Final-Rule-Jan-17-2020.pdf.

flows, both in the United States and overseas, and urge allies to immediately enhance their regulatory capabilities to screen for adversarial capital in sectors critical to national security. It will be necessary to ensure that all countries with advanced technology capabilities have the capacity and ability to process screening requests rapidly, approving appropriate deals while also quickly blocking predatory investments. Speed in both of these areas is particularly important until the world economy is able to reopen.

Recommendation 5: Return - Expand U.S. and Allied Production of Critical Goods

COVID-19 has revealed several areas where the United States depends heavily on foreign supply chains for key goods, including medical supplies and PPE. This challenge will only increase as long-term strategic competition with China spawns spirited contests for more and more markets and industries, especially along the AI supply chain.[49] In response to this challenge, NSCAI offered initial recommendations in Q1 laying the groundwork for the United States' long-term access to resilient, assured microelectronics for its AI advantage.[50] COVID-19 has only heightened the urgency of adopting those Q1 recommendations. But microelectronics is just one component of the full AI supply chain. In other areas, such as rare earth elements, the United States Government is already taking actions to strengthen the domestic industrial base and supply chain.[51] But, in a broad sense, there are areas where the Federal Government needs more information about domestic advanced technology production. To that end, **the Congress should establish a unit within the National Institute of Standards and Technology charged with understanding U.S. capabilities and gaps in domestic advanced technology production.**[52]

---

[49] Michael Brown et al., *Preparing the United States for the Superpower Marathon with China*, Brookings Inst. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_superpower_marathon_brown_chewning_singh.pdf.

[50] *First Quarter Recommendations*, NSCAI (Mar. 2020), https://www.nscai.gov/reports.

[51] *Defense Production Act Title III Presidential Determinations to Strengthen the Domestic Industrial Base and Supply Chain for Rare Earth Elements*, Dept. of Defense, Industrial Policy (Jul. 23, 2019), https://www.businessdefense.gov/News/News-Display/Article/1913110/defense-production-act-title-iii-presidential-determinations-to-strengthen-the/; Timothy Puko, *Pentagon Invests in Strategic Metals Mine, Seeking to Blunt Chinese Dominance*, Wall Street Journal (Apr. 26, 2020), https://www.wsj.com/articles/pentagon-invests-in-strategic-metals-mine-seeking-to-blunt-chinese-dominance-11587924001?mod=searchresults&page=1&pos=4.

[52] Robert D. Atkinson, *The Case for a National Industrial Strategy to Counter China's Technological Rise*, Information Technology & Innovation Foundation, (Apr. 13, 2020), https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise [hereinafter Atkinson, The Case for a National Industrial Strategy].

Understanding the gaps is just the first step. Next, the United States Government must prioritize across industries and create incentives for firms to begin shifting their supply chains. Japan is already taking action in this area by creating a $2 billion fund to subsidize companies to shift production from China back to Japan or into third countries.[53] The Congress should **create a similar incentive fund to provide financial support for firms in critical industries to relocate production now in China to the United States or allied nations.**[54] In addition to direct funding, the United States Government could also use tax breaks,[55] procurement guarantees, and other incentives to ensure that there is sufficient capacity to make select, critical items at secure facilities in the United States and in allied countries.[56]

Finally, the United States should incentivize firms to conduct R&D of critical, advanced technologies in the United States by expanding the existing R&D tax credit as it pertains to technologies deemed essential to U.S. national security, to include AI. Although companies across a wide range of technical and scientific fields are currently eligible for U.S. R&D tax credits, increasing the credits available for companies working in critical, targeted sectors or technologies would prompt increased private sector R&D.[57] Using the tax code to incentivize increased domestic investment in R&D in these sectors will help the elements of the U.S. technology ecosystem most important to national security weather this crisis, and ensure that it is best positioned to maintain global leadership in the years following the pandemic.

---

[53] Isabel Reynolds & Emi Urabe, *Japan to Fund Firms to Shift Production Out of China*, Bloomberg (Apr. 8, 2020), https://www.bloomberg.com/news/articles/2020-04-08/japan-to-fund-firms-to-shift-production-out-of-china.

[54] Atkinson, The Case for a National Industrial Strategy.

[55] One specific proposal would stop the scheduled 2022 expiration of full and immediate expensing of research and development costs. See American Innovation and Competitiveness Act of 2019, H.R. 4549, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4549?s=1&r=6.

[56] Friedberg, Partial Disengagement.

[57] There is substantial evidence that tax incentives can induce growth in private R&D expenditures; when Canada expanded its Scientific Research and Experimental Development to include smaller firms in 2004, it was associated with a 17 percent increase in R&D spending among such firms. See Ajay Agrawal et al., *Tax Credits and Small Firm R&D Spending*, American Economic Journal: Economic Policy (May 2020), https://pubs.aeaweb.org/doi/pdfplus/10.1257/pol.20140467.


NATIONAL
SECURITY
COMMISSION
ON ARTIFICIAL
INTELLIGENCE