Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Cybersecurity for Innovative Small and Medium Enterprises and Academia

Franklin D. Kramer, Melanie J. Teplinsky, and Robert J. Butler

GLOBAL CHINA HUB

CYBER STATECRAFT
INITIATIVE

The Atlantic Council's **Global China Hub** is a new program that researches and devises allied solutions to the three greatest global challenges posed by China's rise: 1) China's rising political, economic, and informational influence on countries, institutions, and global order; 2) the ramifications of an increasingly repressive China under Xi Jinping for open societies and the global economy; and 3) China's drive for dominance in emerging technologies and the prospects for expanding digital authoritarianism globally.

The Global China Hub also strives to amplify and strategically expand the Atlantic Council's body of work on China by leveraging our values, extensive global network, and capacity for integrating insights and information across our 14 other programs and centers. In doing so, the Hub capitalizes on the Council's unique capacity to ascertain "ground truth" on China's trajectory and global impact and to galvanize creative policy solutions among US and allied government stakeholders.

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.

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

Cybersecurity for Innovative Small and Medium Enterprises and Academia

Franklin D. Kramer, Melanie J. Teplinsky, and Robert J. Butler

ISBN-13: 978-1-61977-210-6

January 2022

Contents

Executive Summary

Innovation is fundamental to United States global leadership, critical both for the economy and for national security. Yet the resilience of the US innovation ecosystem against adversary cyber espionage and attack—most specifically from China—has not received the attention required, particularly given the essential innovation roles played by small and medium-sized enterprises (SMEs) and by academia. In response to that challenge, this report sets forth a proposal for expert-provided cybersecurity resilient architectures for SMEs and academia that are engaged in the development and operation of key emerging and advanced technologies. Such cybersecurity resilient architectures would be operated by the private sector and funded through the establishment of transferable cybersecurity investment tax credits. The use of such architectures for the protection of emerging and advanced technologies would play a key role in ensuring that the United States maintains its worldwide innovation leadership.

I. The Challenge

In an era of great power competition, innovation "will play a critical role in defining the national security posture and competitive position" of the United States, according to a 2018 joint report of the Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI).[1] As the Council on Foreign Relations has stated: "Countries that can harness the current wave of innovation, mitigate its potential disruptions, and capitalize on its transformative power will gain economic and military advantages over potential rivals."[2] Likewise, in a recent report to Congress, the Department of Defense (DOD) identified the national security innovation base[3] as critical to the success of the military's effort to meet the "complex warfighting challenges posed by advanced technologies in the [twenty-first] century, from AI [artificial intelligence] to cyber to hypersonics and autonomous air and sea systems."[4]

> "The main challenge to the United States' leadership in innovation is China, whose activities include a significant amount of illegal technological and intellectual property (IP) acquisitions. . . Of particular concern is China's cyber-enabled theft of intellectual property."

The main challenge to the United States' leadership in innovation is China, whose activities include a significant amount of illegal technological and intellectual property (IP) acquisitions. Federal Bureau of Investigation (FBI) Director Christopher Wray has stated that China is "determined to steal its way up the economic ladder,"[5] having "pioneered a societal approach to stealing innovation any way it can from a wide array of businesses, universities, and organizations."[6] More recently, he described: "What we've seen is that it takes the full range of our resources to battle the threat to innovation. . . . Most of the time, that threat is coming from the Chinese government or companies under its sway. And to say they're well-resourced is an understatement. No company is armed to defend against that kind of multi-avenue threat alone."[7] Similarly, a former US assistant attorney general for national security, John Demers, put it this way: "China is using cyberintrusions as part of its rob, replicate, and replace strategy to technological development."[8] The combination of China's IP theft,

1 Department of Homeland Security/Office of the Director of National Intelligence, Analytic Exchange Program, *Emerging Technology and National Security*, July 26, 2018, https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf.

2 Council on Foreign Relations, *Innovation and National Security: Keeping Our Edge*, Updated September 2019, ("*Keeping Our Edge*"), https://www.cfr.org/report/keeping-our-edge/.

3 The phrase "national security innovation base" refers to "the American network of knowledge, capabilities, and people—including academia, National Laboratories, and the private sector—that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life. The genius of creative Americans, and the free system that enables them, is critical to American security and prosperity." White House, *National Security Strategy of the United States of America,* December 2017, 21, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

4 Office of the Secretary of Defense, *FY20 Industrial Capabilities Report to Congress*, 13, https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.

5 "A Conversation with Christopher Wray," Council on Foreign Relations (event), April 26, 2019, https://www.cfr.org/event/conversation-christopher-wray-0. Indeed, roughly 90 percent of the Justice Department's economic espionage cases from 2011 to 2018 involved China. See Keynote Remarks as Prepared for Delivery, National Counterintelligence and Security Center Director William Evanina, International Legal Technology Association LegalSEC Summit 2019, https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.

6 "A Conversation with Christopher Wray."

7 Christopher Wray, "Working with Our Private Sector Partners to Combat the Cyber Threat," Speech as Delivered, Federal Bureau of Investigation (website), October 28, 2021, https://www.fbi.gov/news/speeches/working-with-our-private-sector-partners-to-combat-the-cyber-threat-wray-ecny-102821.

8 Brian Barrett, "Chinese Hackers Charged in Decade-Long Crime and Spying Spree," *Wired*, July 21, 2020, https://www.wired.com/story/chinese-hackers-charged-decade-long-crime-spying-spree/.

and its state-driven industrial policies,[9] poses a significant threat to US economic and national security.

Of particular concern is China's cyber-enabled theft of intellectual property. The US intelligence community has assessed that China presents "a prolific and effective cyber-espionage threat."[10] As *The Economist* put it, "[f]or all the attention devoted to the Taiwan Strait and trade tariffs, cyber-espionage may be the most active mode of conflict between China and America . . . for years to come."[11]

The Cybersecurity and Infrastructure Security Agency (CISA) of DHS has determined that China's "cyber-espionage operations and coordinated theft of information and technology places US government, CI [critical infrastructure], and private industry organizations at risk of loss of sensitive data and technology, trade secrets, intellectual property, and PII [personally identifiable information]."[12] In October 2020, the National Security Agency (NSA) issued an advisory specifically warning that Chinese state-sponsored actors were "exploit[ing] computer networks of interest that hold sensitive intellectual property, economic, political, and military information."[13]

According to the US intelligence community, "China's cyber-espionage operations have included compromising telecommunications firms, providers of managed services and broadly used software, and other targets potentially rich in follow-on opportunities for intelligence collection, attack, or influence operations."[14] Other important sectors targeted by Chinese espionage include semiconductor companies, medical institutions, universities, and the defense industrial base.[15] Small businesses have been among the entities attacked.[16] In July 2021, the United States and several allies, partners, and NATO, issued coordinated statements attributing to China "multiyear campaign[s] targeting foreign governments and entities in key sectors, including maritime, aviation, defense, education, and healthcare in at least a dozen countries."[17] A Department of Justice (DOJ) indictment that was issued simultaneously described China's campaign to hack into the computer systems of dozens of companies, universities, and government entities in the United States to obtain information of "significant economic benefit to China's companies and commercial sectors, including information that would allow the circumvention of lengthy and resource-intensive research and development processes."[18] The National

9 Industrial policies of particular note:
(a) China "divert[s] emerging technologies to military programs" through so-called military-civil fusion. See White House, *National Strategy for Critical and Emerging Technologies*, October 2020, 1, https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf; see also, US Department of State, *Military-Civil Fusion and the People's Republic of China;*
(b) China's National Intelligence Law requires Chinese entities to "share technology and information with military, intelligence, and security services." See ODNI, *Annual Threat Assessment of the US Intelligence Community*, April 9, 2021, 20. Specifically, Article 7 of China's National Intelligence Law states: "Any organization or citizen shall support, assist, and cooperate with state intelligence work in accordance with the law, and maintain the secrecy of all knowledge of state intelligence work." Referenced in Evanina's keynote remarks (see footnote 5); Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare* (blog), Lawfare Institute in cooperation with the Brookings Institution, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Translations: National Intelligence Law of the People's Republic of China, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf; see also https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/; and
(c) China "target[s] sources of United States and allied strength by . . . stealing technology, coercing companies to disclose intellectual property, undercutting free and fair markets, [and] failing to provide reciprocal access in research and development (R&D)." See White House, *National Strategy for Critical and Emerging Technologies*, 1.

10 ODNI, *Annual Threat Assessment of the US Intelligence Community*, (ATA 2021), April 9, 2021, 8; see also Cybersecurity and Infrastructure Security Agency (CISA), "Chinese Cyber Threat Overview and Actions for Leaders," *CISA Insights*, July 19, 2021, https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Chinese_Cyber_Threat_Overview_for_Leaders-508C.pdf#page=1.

11 "Chinese Cyber-attacks—Ctrl-alt-denounce—After Failing to Dissuade Cyber-attacks, America Looks to its Friends for Help," *Economist,* July 20, 2021, https://www.economist.com/united-states/2021/07/20/america-and-its-allies-admonish-but-do-not-punish-china-for-hacking.

12 CISA, "Chinese Cyber Threat Overview and Actions for Leaders."

13 National Security Agency Cybersecurity Advisory, "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities," 1, https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF#page=1.

14 ATA 2021, 8; see also, CISA, "Chinese Cyber Threat Overview and Actions for Leaders."

15 CISA, "Chinese Cyber Threat Overview and Actions for Leaders."

16 "At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software," March 5, 2021, *Krebs on Security* (blog), https://krebsonsecurity.com/tag/hafnium/.

17 "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," White House, Briefing Room Statements and Releases (website), July 19, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

18 US Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," DOJ News Release, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion; See also, *Worldwide Threats Hearing before the US Senate Committee on Homeland Security and Governmental Affairs*, 117th Cong. 6 (2021) (statement of Christopher A. Wray, Director of the Federal Bureau of Investigation), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2021-09-21-REVISED.pdf. Wray described a Chinese "campaign to hack into the computer systems of dozens of victims while trying to obtain information with significant economic benefit" to China.

Counterintelligence and Security Center recently stated, "American technological dominance is under threat by strategic competitors like the PRC . . . [including] the threats posed by cyberattacks . . . [to] steal our data. . . ."[19]

China's cyberespionage operations frequently target academia, including professors, research scientists, and graduate students. FBI Director Wray has specifically warned universities to guard against the China threat, including Chinese efforts to "steal innovation" via graduate students and researchers.[20] According to Wray: "They seek our cutting-edge research, our advanced technology, and our world-class equipment and expertise." [21] As a 2019 Senate staff report warned: "The US academic community is in the crosshairs of not only foreign competitors contending for the best and brightest, but also of foreign nation states that seek to transfer valuable intellectual capital and steal intellectual property."[22]

The US government has been active in raising awareness of the academic espionage threat in a variety of fora for some time. Congressional hearings (e.g., exploring the nexus between China's talent recruitment plans and economic espionage),[23] testimony,[24] and reports[25] repeatedly have broached the subject. In recent years, US law enforcement and intelligence officials have directly warned the leaders of research universities regarding cybersecurity and espionage threats.[26]

The research and educational missions of academia generally incline its institutions toward the very openness and collaboration which render academia particularly vulnerable to espionage. Experts have called for various measures including funding transparency, enhanced background checks, and management of risks associated with collaboration (through oversight regarding travel and workflow, for instance),[27] to safeguard the US research enterprise in the face of the academic espionage threat.[28] In pursuit of the same goal, the National Science and Technology Council (NSTC), after consulting with numerous universities,[29] developed a set of research security guidelines designed to "strengthen and protect the security and integrity of America's research enterprise," including universities.[30] FBI officials reportedly visited numerous research universities in 2019, advising them to "monitor students and scholars associated with . . . an unclassified list of Chinese research institutions and companies."[31]

US government warnings about Chinese academic espionage have met a variety of responses from academia, including skepticism over the gravity of the threat; concern regarding academia's lack of available resources to

19 National Counterintelligence and Security Center, "Protecting US Critical and Emerging Technologies from Foreign Threats," Fact Sheet, October 2021, 4, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf. PRC stands for the People's Republic of China.

20 "A Conversation with Christopher Wray"; see also Brendan O'Malley, "FBI Chief Warns Universities to Guard against China Threat," *University World News*, May 4, 2019, https://www.universityworldnews.com/post.php?story=20190503145355529. ("Christopher Wray, director of the [FBI], has warned universities in the United States to think more carefully about the 'generational threats' posed by China, including its attempts to 'steal innovation' via graduate students and researchers**,**" according to the report.)

21 "A Conversation with Christopher Wray."

22 See, e.g., US Senate Comm. on Homeland Security and Governmental Affairs (HSGAC) Permanent Subcomm. on Investigations, *Threats to the US Research Enterprise: China's Talent Recruitment Plans*, Staff Report, November 19, 2019, 5, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf.

23 *Hearings on Securing the US Research Enterprise from China's Talent Recruitment Plans before the Senate Comm. on Homeland Security and Governmental Affairs Permanent Subcomm. on Investigations*, November 19, 2019, https://www.hsgac.senate.gov/subcommittees/investigations/hearings/securing-the-us-research-enterprise-from-chinas-talent-recruitment-plans.

24 See, e.g., *Hearings on Student Visa Integrity before the Senate Judiciary Comm. Subcomm. on Border Security and Immigration*, 115th Cong. 3 (June 6, 2018) (statement of E.W. Priestap, Assistant Director of the Counterintelligence Division, FBI), https://www.judiciary.senate.gov/imo/media/doc/06-06-18%20Priestap%20Testimony.pdf. ("US academic environments offer valuable, vulnerable, and viable targets for foreign espionage . . . [that some foreign visitors exploit] by stealing "unpublished data, laboratory designs, grant proposals, experiment processes, research samples, blueprints, and state-of-the-art software and hardware." Priestap also warned about the "use of foreign academics by their home countries' intelligence services" seeking "access to sensitive research and export-restricted hardware, and an opportunity to spot recruits for clandestine operations.")

25 See, e.g., US Senate HSGAC Permanent Subcomm. on Investigations, *Threats to the US Research Enterprise*, 5.

26 Emily Feng, "FBI Urges Universities to Monitor Some Chinese Students and Scholars in the U.S.," *All Things Considered*, NPR, June 28, 2019, https://www.npr.org/2019/06/28/728659124/fbi-urges-universities-to-monitor-some-chinese-students-and-scholars-in-the-u-s. Feng reported that intelligence officials "briefed about seventy college administrators of the American Council on Education."

27 Suzanne Folsom and Robert Garretson, "The Continuing Danger of Academic Espionage," *Inside Higher Ed*, May 5, 2020, https://www.insidehighered.com/views/2020/05/05/threat-academic-espionage-should-not-be-overlooked-even-time-pandemic-opinion.

28 Folsom and Garretson, "The Continuing Danger of Academic Espionage."

29 Alexandra Witze, "Trump's Top Scientist Outlines Plan to Reduce Foreign Influence on US Research," *Nature*, September 17, 2019, https://www.nature.com/articles/d41586-019-02787-y.

30 Subcommittee on Research Security, National Science and Technology Council (NSTC) Joint Committee on the Research Environment (JCORE), *Recommended Practices for Strengthening the Security and Integrity of America's S&T Research Enterprise*," Executive Office of the President of the United States, January 2021, 1, https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf**.**

31 Feng, "FBI Urges Universities to Monitor."

counter it; and concerns that xenophobia and racial profiling may inappropriately animate initiatives ostensibly designed to address Chinese academic espionage.[32] While broad US government efforts to stem academic espionage from China have not been without controversy (particularly due to their effects on researchers of Chinese descent and potential chilling effects on universities),[33] focused efforts to staunch the Chinese cyberespionage threat to academia, such as those described in this paper, do not raise such concerns.

As one example of the multiyear cyberespionage campaign described above, Chinese hackers allegedly targeted more than two dozen universities in the United States, Canada, and Southeast Asia to steal maritime-technology research developed for military use.[34] The hacking group had been active since at least 2013,[35] and historically had shown interest in targets "connected to South China sea issues."[36] The hacking group "focused on maritime-related targets across multiple verticals," including research universities, with victims, including the Massachusetts Institute of Technology (MIT) and other academic institutions, mostly in the United States.[37] Similarly in 2015, DOD warned that hackers "affiliated with a known foreign intelligence agency" were targeting academic institutions, just weeks after the University of Virginia learned that Chinese hackers were targeting its China experts with ties to the US intelligence community.[38]

The impact of cyber espionage, which "accounts for a majority . . . of IP theft,"[39] is substantial. General Keith Alexander, former director of the National Security Agency and commander of US Cyber Command, has stated that the value of IP loss via cyberespionage constitutes the "greatest transfer of wealth in history."[40] DOD estimates that "America loses nearly $450 billion on an annual basis to cyber hacking, which originates overwhelmingly from China. This behavior already has severely damaged the Department of Defense and its prime contractors, from stolen plans for major weapons systems such as the F-35, to identity theft from America's defense and security workforce."[41] Other estimates place US losses "between $20 billion and $30 billion annually from Chinese cyber espionage for decades."[42]

The economic impact of China's cyber theft of intellectual property extends beyond direct monetary losses. Chinese IP theft reduces US exports, potentially translating to thousands of lost jobs.[43] Moreover, "[h]aving spent less on innovation, Chinese firms have more resources available for production. If the sector in question is deemed valuable by the central or local government, firms will receive heavy

32 Amy Qin, "As U.S. Hunts for Chinese Spies, University Scientists Warn of Backlash," *New York Times*, November 28, 2021, https://www.nytimes.com/2021/11/28/world/asia/china-university-spies.html. ("Nearly 2,000 academics at institutions including Stanford University, the University of California, Berkeley, and Princeton University have signed open letters to Attorney General Merrick Garland expressing concerns that [some law enforcement efforts to stem academic espionage from China] disproportionately target researchers of Chinese descent.")

33 Amy Qin, "As U.S. Hunts for Chinese Spies," (describing a "chilling effect" that reportedly has "slowed research" and "contributed to a flow of talent out of the United States").

34 Dustin Volz, "Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets," *Wall Street Journal*, March 5, 2019, https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800; see also Mandiant Inc. (formerly FireEye), "Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting US Engineering and Maritime Industries," March 16, 2018, https://www.mandiant.com/resources/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.

35 Security researchers have dubbed the hacking group Leviathan, APT 40, and TEMP.Periscope, among other names. US Department of Justice, "Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," DOJ Office of Public Affairs Release, July 19, 2021, https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion.

36 Ionut Arghire, "China-linked Hackers Target Engineering and Maritime Industries," *Security Week*, March 16, 2018, https://www.securityweek.com/china-linked-hackers-target-engineering-and-maritime-industries.

37 Mandiant Inc. (formerly FireEye), "Suspected Chinese Cyber Espionage Group."

38 Katie Bo Williams, "University of Virginia Hack Targeted Employees with China Ties," *Hill*, August 21, 2015, https://thehill.com/policy/cybersecurity/251643-uva-hack-targeted-individuals-with-china-ties; see also Shane Harris and Alexa Corse, "Chinese Hackers Target US University with Government Ties," *Daily Beast*, August 21, 2015, Updated April 14, 2017, https://www.thedailybeast.com/chinese-hackers-target-us-university-with-government-ties; and FBI, "China: The Risk to Academia," 2019, 10, https://www.fbi.gov/file-repository/china-risk-to-academia-2019.pdf. The FBI noted that a China-based threat actor with a history of targeting victims in aerospace, defense, and academia compromised the network at the College of Engineering of a large northeastern state university, likely in search of sensitive information and IP.

39 James Andrew Lewis, "How Much Have the Chinese Actually Taken?," Center for Strategic and International Studies, March 22, 2018, https://www.csis.org/analysis/how-much-have-chinese-actually-taken.

40 *Hearings on the Future of Warfare before the Senate Armed Services Comm.*, 114th Cong. 3 (November 3, 2015) (statement of General [Ret.] Keith Alexander, former Director of the National Security Agency and former Commander, United States Cyber Command), https://www.armed-services.senate.gov/imo/media/doc/Alexander_11-03-15.pdf.

41 Office of the Secretary of Defense, *FY20 Industrial Capabilities Report to Congress*, January 2021, 12, https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.

42 Lewis, "How Much Have the Chinese Actually Taken?"

43 Lewis, "How Much Have the Chinese Actually Taken?" ("Chinese IP theft reduced US exports, meaning the United States could have lost thousands of jobs annually. 'Lost' is an inaccurate term, since the 'net' employment loss can be smaller if workers displaced by IP theft find other jobs. Yet these new positions can pay less, since IP theft can shift employment away from high-paying jobs.")

CHINESE CYBERESPIONAGE OF HIGH TECH INTELLECTUAL PROPERTY

Chinese cyberoperations targeting US COVID-19 vaccines and other high tech research[1]

Two Chinese hackers allegedly working with China's Ministry of State Security (MSS) were indicted on July 2020,[2] allegedly having "probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines, testing technology, and treatments"; and conspired to steal trade secrets "including technology designs, manufacturing processes, test mechanisms and results, source code, and pharmaceutical chemical structures."[3] The hackers allegedly "conducted a hacking campaign lasting more than ten years . . . targeting companies in countries with high technology industries, including the United States. . . . Targeted industries included, among others, high tech manufacturing; medical device, civil and industrial engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense."[4] The targeted information would give Chinese competitors "a market edge by providing insight into proprietary business plans and savings on research and development costs in creating competing products."[5]

1 FBI, "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations," FBI National Press Office Release, May 13, 2020, https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations.

2 United States v. Li Xiaoyu and Dong Jiazhi, 4:20-CR-6019-SMJ, (E.D. Wash.), July 7, 2020, https://www.justice.gov/opa/press-release/file/1295981/download.

3 US Department of Justice, "Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research," July 21, 2020, https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

4 US Department of Justice, "Two Chinese Hackers."

5 US Department of Justice, "Two Chinese Hackers."

subsidies. As a result, they can underprice foreign competitors, driving these competitors first out of the [People's Republic of China], then out of overseas markets. Legal and illegal technology acquisition followed by enormous state support helps account for the speed and extent of the rise of Chinese telecom-equipment makers, for example."[44]

Similarly, cyber-enabled nation-state theft of sensitive data from the defense industrial base (DIB) poses a significant threat to national security and has been well-documented for over a decade.[45] In 2011, after 24,000 terabytes of data had been exfiltrated from a large DOD contractor, then-Deputy Defense Secretary William Lynn stated: "It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies."[46] Today, "[t]he DIB continues to hemorrhage critical data."[47] DOD recently warned Congress that the DIB is "subject to continuous, coordinated cyberattack campaigns by nation states," and specifically called out China for "Beijing's ongoing activities as the world's most egregious cyber threat and intellectual property (IP) thief."[48]

44 Derek Scissors, "The Rising Risk of China's Intellectual-Property Theft," *National Review*, July 15, 2021, https://www.nationalreview.com/magazine/2021/08/02/the-rising-risk-of-chinas-intellectual-property-theft/.

45 See e.g., Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011, https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf; and Mandiant, *APT1: Exposing One of China's Cyberespionage Units*, March 13, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

46 Chris Lefkow, "24,000 Files Stolen from Defense Contractor: Pentagon," PHYS.org (news aggregator), July 15, 2011, http://phys.org/news/2011-07-stolen-defense-contractor-pentagon.html.

47 Secretary of the Navy, *Cybersecurity Readiness Review*, March 2019, 43, https://www.hsdl.org/?abstract&did=823225.

48 Office of the Secretary of Defense, *Fiscal Year 2020 Industrial Capabilities Report to Congress*, January 2021, 12, https://media.defense.gov/2021/Jan/14/2002565311/-1/-1/0/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.

II. The Importance of Protecting SMEs and Academia

A. SMEs

SMEs are significant generators of innovation across all US industry sectors.[49] For example, small companies are "overwhelmingly driving innovation" in pharmaceuticals, "accounting for 63 percent of all new prescription drug approvals over the past five years."[50] Similarly, small biotechnology companies "hold approximately 80 percent of the development pipeline for new medicines, diagnostics and other bio-based products."[51] Likewise, SMEs are essential "engines of innovation and vitality,"[52] especially for the US defense industrial base, or DIB, and the national security innovation base (NSIB). In fact, SMEs comprise nearly three-quarters of the DIB and nearly all firms in the third and fourth tiers of the DIB supply chain.[53] SMEs perform nearly 20 percent of overall research and development (R&D) in the United States and the EU, and file more than 35 percent of transnational patents.[54] Small businesses develop more "patents per employee" than large firms, and their patents outperform large firm patents with respect to "growth, citation impact, and originality."[55]

Many of today's most innovative companies began as SMEs. In the IT sector, these companies include household names such as Google,[56] Facebook,[57] Microsoft,[58] Apple,[59] Amazon,[60] Oracle,[61] Dell,[62] and Cisco,[63] as well

> "Small businesses develop more 'patents per employee' than large firms, and their patents outperform large firm patents with respect to 'growth, citation impact, and originality.'"

49 SMEs account for over 40 percent of the US private payroll and drive both innovation and competitiveness. Before the pandemic, small businesses with fewer than 500 employees accounted for two-thirds of net new American jobs. See Maneet Ahuja, "Small Business Strikes Back: The Numbers Behind the Next 1000," *Forbes*, February 16, 2021, https://www.forbes.com/sites/maneetahuja/2021/02/16/small-business-strikes-back-the-numbers-behind-the-next-1000/?sh=63a9461a5fd4; US Small Business Administration (SBA) Office of Advocacy, "Small Businesses Generate 44% of US Economic Activity," January 30, 2019, https://advocacy.sba.gov/2019/01/30/small-businesses-generate-44-percent-of-u-s-economic-activity/; and SBA Office of Advocacy, Frequently Asked Questions (SBA website), https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf.

50 Pharmaceutical companies make medicine from chemicals and synthetic processes in contrast to biotechnology companies, which make medicines from living organisms. Regarding drug approvals, see Robin Robinson, "Small Pharma Driving Big Pharma Innovation," *PharmaVOICE*, January 2020, 14, https://www.pharmavoice.com/article/2020-01-pharma-innovation/.

51 *Public Hearing on the Study of International Patent Protection for Small Businesses before the United States Patent and Trademark Office* 81:8-10 (October 27, 2011) (statement of Stanley Erck, CEO of Novavax), https://www.uspto.gov/sites/default/files/aia_implementation/111027-ipsb_transcript.pdf; see also Robinson, "Small Pharma Driving Big Pharma Innovation."

52 *Hearing to Receive Testimony on the Cybersecurity of the Defense Industrial Base before the US Senate Comm. on Armed Services Subcomm. on Cybersecurity* (Transcript, May 18, 2021, 36) (testimony of Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy), https://www.armed-services.senate.gov/imo/media/doc/21-39_05-18-2021.pdf.

53 See *Hearing on the Cybersecurity of the Defense Industrial Base before the US Senate Comm. on Armed Services Subcomm. on Cybersecurity* (May 18, 2021) (statement of Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy), https://www.armed-services.senate.gov/imo/media/doc/DASD%20Salazar%2020210518_CMMC%20Hearing%20-%20FINAL1.pdf#page=2

54 Organisation of Economic Co-operation and Development and the International Energy Agency (IEA), *Accelerating Energy Efficiency in Small and Medium-Sized Enterprises: Powering SMEs to Catalyse Economic Growth*, IEA Publication, 2015, 13, https://c2e2.unepdtu.org/wp-content/uploads/sites/3/2016/03/sme-2015.pdf.

55 Anthony Breitzman and Diana Hicks, "An Analysis of Small Business Patents by Industry and Firm Size," *Faculty Scholarship for the College of Science and Mathematics,* Rowan University, November 2008, https://rdw.rowan.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1011&context=csm_facpub.

56 Google was born when two Stanford University students built a search engine from their dorm rooms. Google now makes "hundreds of products used by billions of people across the globe," according to its website, https://about.google/our-story/.

57 Nicholas Carlson, "At Last—the Full Story of How Facebook Was Founded," *Business Insider,* March 5, 2010, https://www.businessinsider.com/how-facebook-was-founded-2010-3.

58 Start-up computer software maker Microsoft grew into a major multinational technology corporation. Mary Bellis, "A Short History of Microsoft," *ThoughtCo*, Updated January 10, 2020, https://www.thoughtco.com/microsoft-history-of-a-computing-giant-1991140.

59 Nik Rawlinson, "History of Apple: The Story of Steve Jobs and the Company He Founded," *MacWorld*, April 25, 2017, https://www.macworld.co.uk/feature/history-of-apple-steve-jobs-mac-3606104/.

60 Avery Hartmans, "Jeff Bezos Originally Wanted to Name Amazon 'Cadabra,' and 14 Other Little-known Facts about the Early Days of the E-commerce Giant," *Business Insider*, July 2, 2021, https://www.businessinsider.com/jeff-bezos-amazon-history-facts-2017-4#amazon-wasnt-the-companys-original-name-1.

61 Avery Hartmans, "The Life and Career of Larry Ellison, the Billionaire Oracle Cofounder Who Went from College Drop-Out to Jet-Setting Playboy and Tech Titan," *Business Insider,* updated April 1, 2021, https://www.businessinsider.com/rise-of-oracle-founder-larry-ellison-2017-1.

62 Dell Technologies Timeline, Dell (website) https://corporate.delltechnologies.com/en-us/about-us/who-we-are/timeline.htm.

63 "Who Is Cisco," Cisco (website), https://www.cisco.com/c/en_au/about/who-is-head.html.

as leading cybersecurity firms such as CrowdStrike,[64] Mandiant,[65] FireEye,[66] Palo Alto Networks,[67] and Tenable.[68] Industry-leading semiconductor firm Nvidia, which designs graphics processing units used for accelerated computing, was started with $40,000 and is now valued at over $650 billion, making it one of the 10 largest companies in the United States by market capitalization.[69]

In other sectors, Moderna Therapeutics grew from a small start-up biotechnology company to a company with a market capitalization of well over $100 billion as investors realized the value of the mRNA technology underlying its COVID-19 vaccine.[70] Mitchell Energy revolutionized the energy sector in the late 1990s through the implementation of fracking,[71] an efficient method of unlocking natural gas from shale; the business ultimately sold for $3.1 billion.[72] Aurora Flight Sciences—founded in 1989 as a small Virginia-based aeronautics research company—has become known for its innovative autonomous aircraft and was acquired by Boeing in 2017.[73] Tesla, founded in 2003 to develop an electric sports car,[74] has since brought to market the first zero-emission full-size electric vehicle, and manufactures battery packs, motors, and other components capable of powering its own and other manufacturers' electric vehicles.[75] Notably, the US Department of Energy loaned $465 million to Tesla in 2010 (which was fully repaid in 2013) to support "commercial-scale deployment of advanced technologies that help keep American auto manufacturers competitive in the growing global market for advanced vehicles."[76] Tesla's market capitalization recently exceeded $1 trillion.

B. Academia

Academia also plays a key role in technological innovation. Academic technology transfer is estimated to have contributed $1.7 trillion to US gross industrial output; contributed more than $865 billion to US gross domestic product; and supported 5.9 million jobs since 1996.[77] A host of familiar innovations—including cell phone technologies,[78] the key filtration technology used in N95 respirators,[79] the nicotine

64 "CrowdStrike Holdings, Inc.," Left Brain Investment Research, https://static1.squarespace.com/static/5c3a4bd3b27e39b123503621/t/5f936a718dac6b256d9b0ec5/1603496563620/Crowdstrike+-+Fresh+Look+-+10_16_2020.pdf; and "How Success Struck CrowdStrike," Innovation Cybersecurity Ecosystem (ICE) Block71 (a Singapore-based cybersecurity start-up hub), September 30, 2019, https://ice71.sg/how-success-struck-crowdstrike/.

65 During his tenure as CEO of Mandiant, founder Kevin Mandia grew the company "to nearly 500 employees and more than $100 million in revenue," per Cyber Defense Summit Speaker Biography, "Kevin Mandia," https://summit.fireeye.com/learn/speakers/kevin-mandia.html; and see Brian Fung, "Mandiant, Which Rooted Out Chinese Hackers for the NYT, Is Being Snapped Up for Nearly $1 Billion," *Washington Post,* January 2, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/01/02/mandiant-which-rooted-out-chinese-hackers-for-the-nyt-is-being-snapped-up/.

66 "Making the Impossible Possible," *New Spaces*, Toffee TV (product), March 7, 2016 (describing the "start-up phase" of FireEye when founder Ashar Aziz "was working out of his house, had $4,000 in the corporate bank account and some of his personal savings[, and] worked an intense eighty to one-hundred hours week after week"), https://thenewspaces.com/2016/03/07/making-the-impossible-possible-ashar-aziz/.

67 Caleb Melby, "Nir Zuk's Palo Alto Networks Is Blowing Up Internet Security," March 27, 2013, https://www.forbes.com/sites/calebmelby/2013/03/27/nir-zuks-palo-alto-networks-is-blowing-up-internet-security/?sh=14de0c8cff92.

68 Transcript of Interview of Ron Gula, "Why a Failed Fighter Pilot Made a Better Founder (and Took a Company Public)," *Mixergy*, February 27, 2019, https://mixergy.com/interviews/tenable-with-ron-gula/.

69 Emily Bary, "Nvidia Eclipses Warren Buffett's Berkshire Hathaway as 7th Largest US Company," *MarketWatch*, November 2, 2021, https://www.marketwatch.com/story/nvidia-on-track-to-eclipse-warren-buffetts-berkshire-hathaway-as-7th-largest-u-s-company-11635869984.

70 Kelly Servick, "This Mysterious $2 Billion Biotech Is Revealing the Secrets behind Its New Drugs and Vaccines," *Science*, March 25, 2020, https://www.science.org/news/2017/02/mysterious-2-billion-biotech-revealing-secrets-behind-its-new-drugs-and-vaccines.

71 Fracking is drilling and hydraulic fracturing of extremely dense shale. See Gregory Zuckerman, "Breakthrough: The Accidental Discovery That Revolutionized American Energy," *Atlantic*, November 6, 2013, https://www.theatlantic.com/business/archive/2013/11/breakthrough-the-accidental-discovery-that-revolutionized-american-energy/281193/.

72 Zuckerman, "Breakthrough: The Accidental Discovery."

73 Aurora Flight Sciences, https://www.aurora.aero/; and Aaron Gregg, "Boeing Takes Another Step into the Pilotless Plane Market," *Washington Post*, October 5, 2017, https://www.washingtonpost.com/news/business/wp/2017/10/05/boeing-takes-another-step-into-the-pilotless-plane-market/.

74 Stephen Edelstein, "Tesla Existed before Elon Musk: Founders on How They Pitched the Idea," *Green Car Reports*, February 9, 2021, https://www.greencarreports.com/news/1131215_tesla-existed-before-elon-musk-founders-on-how-they-pitched-the-idea.

75 DOE funding played a role in the development of Tesla's batteries and solar panels. See *Keeping Our Edge*, https://www.cfr.org/report/keeping-our-edge/.

76 "Tesla," Department of Energy Loan Programs Office (website), https://www.energy.gov/lpo/tesla.

77 "Driving the Innovation Economy: Academic Technology Transfer in Numbers," AUTM, https://autm.net/AUTM/media/SurveyReportsPDF/AUTM_FY2018_Infographic.pdf; AUTM, "What Is Tech Transfer, Anyway?," https://autm.net/about-tech-transfer/what-is-tech-transfer; Lori Pressman et al., "The Economic Contribution of University/Nonprofit Inventions in the United States: 1996-2015," AUTM, https://autm.net/AUT/media/About-AUTM/Documents/AUTM_BIO_Economic_Impact_Report_2017.pdf; and "4 Ways Universities Are Driving Innovation," World Economic Forum (website), https://www.weforum.org/agenda/2018/01/4-ways-universities-are-driving-innovation/.

78 The "resistive touch screen," for example, was developed by Samuel Hurst at the University of Kentucky in 1971, while the "multicore processing" used in the iPhone since 2009 can be traced to Professor Kunle Olukotun and other Stanford University researchers who developed the first "multicore processor" in 1995. See Association of American Universities, "University Research Made Your Smartphone Smart," September 19, 2017, https://www.aau.edu/university-research-made-your-smartphone-smart. See also Samuel K. Moore, "Multicore CPUs: Processor Proliferation," *IEEE Spectrum*, Institute of Electrical and Electronics Engineers, January 2011, https://spectrum.ieee.org/multicore-cpu-processor-proliferation.

79 In 1992, Peter Tsai led a research team at the University of Tennessee to develop the "electrostatic charging technology [that] . . . eventually became the foundation of the N95 respiratory mask." See Sydney Page, "The Retired Inventor of N95 Masks Is Back at Work, Mostly for Free, to Fight COVID-19," *Washington Post*, July 7, 2020, https://www.washingtonpost.com/lifestyle/2020/07/07/peter-tsai-n95-mask-covid/; and "U Tennessee's Essential N95 Mask Technology Protects Billions," AUTM, https://autm.net/about-tech-transfer/better-world-project/bwp-stories/n95-mask-u-tennessee.

patch,[80] Cochlear implants,[81] Coumadin for treating blood clots,[82] and Allegra for allergy relief[83]—have their origins in university research.[84]

Universities became "hotbeds of innovation"[85] with the passage of the Bayh-Dole Act in 1980.[86] This landmark legislation allowed universities and their faculty to own the patents on, and commercialize inventions resulting from, federally funded research. While not without its critics,[87] the act was "instrumental in encouraging universities to participate in technology transfer activities."[88] In the two decades following its passage, the number of patents generated by US universities increased by a factor of ten; more than 2,200 firms were spun off to take advantage of research done in university labs; and over a quarter of a million jobs were created.[89]

Biotech offers a useful case study of academia's outsized impact on innovation. In significant part, the biotechnology industry "was created from university start-up companies,"[90] as the numbers reflect: 76 percent of biotech companies had a license from a university in 2010, and at least 50 percent of then-existing biotech companies "got their start" because of a university license.[91] Proponents of the Bayh-Dole Act credit it with "academic/industry partnerships that have yielded sixty biotech therapies, including: Herceptin, which is Genentech Inc's breast cancer drug, and Nupogen, [a] remedy for the dip in infection-fighting white blood cells that can result from chemotherapy."[92]

"Biotech offers a useful case study of academia's outsized impact on innovation. In significant part, the biotechnology industry 'was created from university start-up companies,' as the numbers reflect: 76 percent of biotech companies had a license from a university in 2010, and at least 50 percent of then-existing biotech companies 'got their start' because of a university license."

80 Thomas H. Maugh II, "UCLA Pharmacologist Invented Nicotine Patch," *Los Angeles Times*, May 14, 2008, https://www.latimes.com/archives/la-xpm-2008-may-14-me-jarvik14-story.html. (UCLA pharmacologist Murray Jarvik patented the concept of introducing nicotine through a transdermal patch "and assigned the patent to the University of California, which licensed it to Ciba-Geigy, now Novartis. The first prescription nicotine patch reached the market in 1992, and four years later, it became available over the counter.") NicoDerm CQ, "All About the Nicotine Patch," https://www.nicodermcq.com/support-hub/all-about-the-nicotine-patch.html. ("The nicotine patch was first invented by doctors in 1984 at UCLA when they discovered that a transdermal nicotine patch could help people quit smoking.")

81 Albert Mudry and Mara Mills, "The Early History of the Cochlear Implant," *JAMA Network Open* (monthly open access medical journal of the American Medical Association), May 2013, https://jamanetwork.com/journals/jamaotolaryngology/fullarticle/1688121, (which describes the key role of Stanford University and University of California, San Francisco researchers in the development of the cochlear implant); see also AUTM, "Cochlear Implant Brings Sound and Language to Thousands," https://autm.net/about-tech-transfer/better-world-project/bwp-stories/cochlear-implant.

82 AUTM, "UW-Madison Research Yields the Most Widely Prescribed Blood Thinner," AUTM (website) https://autm.net/about-tech-transfer/better-world-project/bwp-stories/coumadin-and-warafin; Ramya Rajagopalan, "A Study in Scarlet," *Science History Institute*, March 29, 2018, https://www.sciencehistory.org/distillations/a-study-in-scarlet, (which details the role of University of Wisconsin biochemist Karl Paul Link in the discovery of the life-saving blood-thinner warfarin, also known by its brand name, Coumadin, and how Warfarin's name came from a combination of Wisconsin Alumni Research Foundation (WARF), which funded Link's work, and coumarin, a natural chemical found in hay that reacts with fungus to make the blood-thinner); and Joe Palca, "How Moldy Hay and Sick Cows Led to a Lifesaving Drug," *All Things Considered*, NPR, August 29, 2017, https://www.npr.org/sections/health-shots/2017/08/29/531749974/how-moldy-hay-and-sick-cows-led-to-a-life-saving-drug.

83 AUTM, "The Birth of Allegra: Nothing to Sneeze At," AUTM (website), https://autm.net/about-tech-transfer/better-world-project/bwp-stories/allegra.

84 Vicki Loise and Ashley J. Stevens, "The Bayh-Dole Act Turns 30," Commentary, *Science Translational Medicine* 2, No. 52 (2010): 2, https://www.science.org/doi/epdf/10.1126/scitranslmed.3001481.

85 "Innovation's Golden Goose," *Economist*, December 14, 2002, https://www.economist.com/technology-quarterly/2002/12/14/innovations-golden-goose.

86 Patent and Trademark Act Amendments of 1980, 35 U.S.C. §§ 200-212 (1980).

87 "Bayhing for Blood or Doling Out Cash?" *Economist*, December 24, 2005, https://www.economist.com/science-and-technology/2005/12/20/bayhing-for-blood-or-doling-out-cash.

88 "Landmark Law Helped Universities Lead the Way," AUTM, https://autm.net/about-tech-transfer/advocacy/legislation/bayh-dole-act.

89 "Innovation's Golden Goose," *Economist*. The article notes that prior to the Bayh-Dole Act, "inventions and discoveries made in American universities, teaching hospitals, national laboratories, and nonprofit institutions sat in warehouses gathering dust. Of the 28,000 patents that the American government owned in 1980, fewer than 5 percent had been licensed to industry." See also a list of more than one hundred innovations made possible by the act in "Bayh-Dole Innovations," AUTM, https://autm.net/about-tech-transfer/advocacy/legislation/bayh-dole-act/bayh-dole-innovations.

90 Loise and Stevens, "The Bayh-Dole Act Turns 30," 2.

91 Loise and Stevens, "The Bayh-Dole Act Turns 30," 2.

92 Bernadette Tansey, "The Building of Biotech/25 Years Later, 1980 Bayh-Dole Act Honored as Foundation of an Industry," *SFGate*, June 21, 2005, https://www.sfgate.com/business/article/The-building-of-biotech-25-years-later-1980-2660978.php.

Technological innovation in academia reaches beyond biotech as academic researchers across the country are driving innovation in multiple key technological areas. Examples include:

- Harvard University research innovations have been at the heart of over 120 new start-up companies over the past decade.[93]

- Northwestern University recently said it will create a "multimillion-dollar technology accelerator to support start-up companies led by Northwestern faculty in health, life sciences, and related fields . . . [enabling] faculty to contribute to innovation through commercialization of sophisticated scientific discoveries."[94]

- Stanford University alumni and faculty are credited with creating nearly 40,000 companies since the 1930s, and the university has produced more technology start-up founders than any other campus, as of 2015.[95] Stanford played a key role in the development of the nation's high-tech hub in Silicon Valley.[96] Through its "innovative medicines accelerator" and a new life sciences incubator, Stanford works to "help basic and applied researchers from across the schools of medicine, engineering and humanities & sciences translate their research discoveries into new therapies and diagnostics."[97]

- MIT researchers are responsible for technological advancements across a variety of fields over the past 150 years.[98] A decade ago, the *Boston Globe* published a list of 150 innovations associated with MIT, including the World Wide Web, RSA public key cryptography, and Bose speakers.[99] More recently, MIT scientists have built neural networks to identify drug combinations likely to be effective against viruses such as HIV and COVID-19, as well as pancreatic cancer; made strides in the development of a salt-based alternative to the ubiquitous lithium-ion battery;[100] and led groundbreaking energy research that eventually could lead to an emissions-free power plant.[101]

- Carnegie Mellon University (CMU) has more than one hundred research centers, many of which focus on key areas such as AI, neuroscience, robotics (through the National Robotics Engineering Center), and cybersecurity (at the Software Engineering Institute).[102] Carnegie Mellon's Center for Technology Transfer and Enterprise Creation fosters efforts to bring CMU research to market.[103]

These programs represent just the tip of the iceberg of innovation in academia.

---

93 "Commercializing Technology," Harvard Office of Technology Development (webpage), accessed December 12, 2021, https://otd.harvard.edu/faculty-inventors/commercializing-technologies/.

94 "Northwestern Plans Multimillion-dollar Technology Accelerator," Northwestern University, Northwestern Now (webpage), August 19, 2021, https://news.northwestern.edu/stories/2021/08/technology-accelerator/.

95 Ritika Trikha, "The Interdependency of Stanford and Silicon Valley," *Tech Crunch*, September 4, 2015, https://techcrunch.com/2015/09/04/what-will-stanford-be-without-silicon-valley/.

96 Trikha, "The Interdependency of Stanford and Silicon Valley."

97 Amy Adams, "New Incubator to Fuel Life Science Innovation in Stanford Research Park," Press Release, Stanford University News Service, September 17, 2019, https://news.stanford.edu/press-releases/2019/09/17/new-incubator-furd-research-park/.

98 "Inventions and innovations," Massachusetts Institute of Technology (webpage), accessed December 12, 2021, https://mitadmissions.org/discover/about-mit/innovations/.

99 Sam Allis et al., "150 Fascinating, Fun, Important, Interesting, Lifesaving, Life-altering, Bizarre and Bold Ways That MIT Has Made a Difference," *Boston Globe,* May 15, 2011, http://archive.boston.com/news/education/higher/specials/mit150/mitlist/?page=full.

100 Anna Powers, "Your Next Battery Could Be Made From Salt, Scientists Make Greener Advances," *Forbes*, January 31, 2020, https://www.forbes.com/sites/annapowers/2020/01/31/your-next-battery-could-be-made-from-salt-scientists-make-greener-advances/.

101 David Chandler, "Validating the Physics behind the New MIT-designed Fusion Experiment," MIT (news website), September 29, 2020, https://news.mit.edu/2020/physics-fusion-studies-0929.

102 "Research" and "Centers and Institutes," Carnegie Mellon University (webpages), accessed December 12, 2021, https://www.cmu.edu/research/index.html and https://www.cmu.edu/research/centers-and-institutes.html, respectively.

103 Carnegie Mellon, "Center for Technology Transfer and Enterprise Creation," accessed December 12, 2021, https://www.cmu.edu/cttec/.

III. Meeting the Cybersecurity Challenge for SMEs and Academia

Protecting critical emerging and advanced technology from cyber espionage and attack is essential if the United States is to maintain its technological leadership. Cybersecurity resilient architectures for SMEs and academia are a key capability necessary to augment existing US government efforts to protect critical technology.

The US government currently utilizes several types of mechanisms to prevent foreign adversary acquisition of critical technologies where such acquisition would threaten US economic or national security.[104] These mechanisms include:

- export controls on dual-use technologies,[105] including efforts to achieve multilateral cooperation on export controls among like-minded democracies to prevent China from acquiring sensitive dual-use technologies;[106]

- limiting dependence on foreign capital through the Committee on Foreign Investment in the United States (CFIUS),[107] merger and acquisition reviews (conducted by DOD,[108] DOJ, and the Federal Trade Commission),[109] and DOD's Trusted Capital (TC) Programs,[110] including the Trusted Capital Digital Marketplace;[111] and

104 This threat is detailed in the National Counterintelligence Strategy: "Foreign intelligence entities have embedded themselves into US national labs, academic institutions, and industries that form America's national innovation base. They have done this to acquire information and technology that is critical to the growth and vitality of the US economy. Adversaries use front companies, joint ventures, mergers and acquisitions, foreign direct investment, and talent recruitment programs to gain access to and exploit US technology and intellectual property. They also influence and exploit US economic and fiscal policies and trade relationships." Office of the Director of National Intelligence, *National Counterintelligence Strategy of the United States of America 2020-2022*, National Counterintelligence and Security Center, 8, https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf.

105 See, e.g., Export Control Reform Act of 2018, 50 U.S.C. §§ 4801-4852, (providing, inter alia, permanent statutory authority for the preexisting dual-use export control system and addressing concerns about the flow of critical technologies to China by requiring the administration to identify—and control the export of—"emerging and foundational technologies" of concern).

106 Sarah Kirchberger and Clementine Starling, "100 Ideas for the First 100 Days—#60: Undertake a Comprehensive Review of Dual-Use Technology Transfers to China," Atlantic Council, March 20, 2021, https://www.atlanticcouncil.org/content-series/100-ideas-for-the-first-100-days/60-undertake-a-comprehensive-review-of-dual-use-technology-transfers-to-china/; Remco Zwetsloot, "The U.S. Needs Multilateral Initiatives to Counter Chinese Tech Transfer," Brookings Institution, June 11, 2020, https://www.brookings.edu/techstream/the-u-s-needs-multilateral-initiatives-to-counter-chinese-tech-transfer/; Cindy Whang, "A Comparative Analysis of the United States and European Union Dual-Use Export Control Regulations," *Security and Human Rights* (2021), https://brill.com/view/journals/shrs/aop/article-10.1163-18750230-31010007/article-10.1163-18750230-31010007.xml?language=en; Ian F. Fergusson and Karen M. Sutter, *U.S. Export Control Reforms and China: Issues for Congress*, Congressional Research Service, In Focus (brief), IF11627, Updated January 15, 2021, https://sgp.fas.org/crs/natsec/IF11627.pdf; and *Hearing on U.S.-China Relations in 2021: "Emerging Risks" before the U.S.-China Economic and Security Review Commission* 4 (September 8, 2021) (statement of Jeremy Pelter, Acting Under Secretary for Industry and Security, Bureau of Industry and Security, US Department of Commerce), https://www.uscc.gov/sites/default/files/2021-08/Jeremy_Pelter_Testimony.pdf.

107 CFIUS is the "US government's principal mechanism for screening foreign investment to assess and address its potential impact on US national security." See David Fagan and Brian Williams, "Intersection of National Security with M&A: The Committee on Foreign Investment in the United States," *Tax Executive*, January 30, 2020, https://taxexecutive.org/intersection-of-national-security-with-ma-the-committee-on-foreign-investment-in-the-united-states/; and US Department of the Treasury, "CFIUS Laws and Guidance," https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-laws-and-guidance.

108 One proposal under the Trusted Capital Program would "allow private investment companies working on technology critical to national security, under certain conditions, to be eligible for preferential tax treatment." See US Department of Defense, "Senior Defense Leaders Brief on Trusted Capital Digital Marketplace," January 13, 2021, https://www.defense.gov/News/Transcripts/Transcript/Article/2473287/senior-defense-leaders-brief-on-trusted-capital-digital-marketplace/.

109 See Hart-Scott-Rodino Antitrust Improvements Act of 1976, 15 U.S.C. § 18a, September 30, 1976, (establishing the federal premerger notification program); see also Office of the General Counsel of the Department of Defense, DOD Directive 5000.62, "Review of Mergers, Acquisitions, Joint Ventures, Investments, and Strategic Alliances of Major Defense Suppliers on National Security and Public Interest," effective February 27, 2017, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/500062p.pdf; Federal Trade Commission (FTC), "Premerger Notification Program," https://www.ftc.gov/enforcement/premerger-notification-program; and FTC, "Joint Statement of the Department of Justice and the Federal Trade Commission on Preserving Competition in the Defense Industry," April 12, 2016, https://www.ftc.gov/system/files/documents/public_statements/944493/160412doj-ftc-defense-statement.pdf.

110 TC is an Undersecretary of Defense for Acquisitions and Sustainment (USD A&S) program "to strengthen the defense industrial base and limit threats to national security posed by adversarial capital." US Department of Defense, "Department of Defense Announces Establishment of the Trusted Capital Digital Marketplace," January 13, 2021, https://www.defense.gov/Newsroom/Releases/Release/Article/2470485/department-of-defense-announces-establishment-of-the-trusted-capital-digital-ma/. TC is a DOD-led whole-of-government approach to support "trusted partnerships between critical capability companies and capital providers." DOD, "Senior Defense Leaders Brief."

111 The Trusted Capital Digital Marketplace (TCDM) established "trusted sources of funding for small and medium-sized providers of innovative defense-critical capabilities, offering long-term strategic benefit and combatting predatory investment practices." See US DOD, "Department of Defense Announces Establishment of the Trusted Capital Digital Marketplace." TCDM basically brings corporate suppliers critical to DIB together with trusted capital providers. In doing so, it supports the DIB and limits adversary nation access to US technology. TCDM serves as a "gateway to an investment ecosystem designed to promote innovation and ensure access to trusted sources of capital for emerging technologies and critical capabilities required for national security.

- limiting dependence on foreign supply chains as the recent executive order on supply chains seeks to achieve.[112]

Cybersecurity resilient architectures, with the requisite financial support, would provide a needed complement to these activities by enhancing cybersecurity resilience for the SME and academic sectors, where market forces have proven insufficient.

There are a number of well-documented reasons for the lack of effective SME cybersecurity.[113] While many SMEs lack understanding and awareness of the cyber threats facing them,[114] the more serious challenge is the cost and complexity of implementing effective cybersecurity. Small firms, including those in the DIB, often lack the necessary resources—including adequate budget, dedicated information technology (IT) staff, and/or experienced personnel—to procure and maintain a robust cyber defense, particularly against sophisticated nation-state adversaries.[115] Many SMEs are below the "security poverty line," a term coined to describe a lack of resources to implement the cybersecurity they need.[116] In a 2019 Cisco survey, only 7 percent of respondents from organizations with between 1,000 and 9,999 employees said they were able to afford the minimum security they needed.[117] Even the most profitable of the small DIB firms are, a RAND Corporation report said, "unlikely to have enough money for all the [cybersecurity tools] they need if they hire and retain the number of recommended cybersecurity personnel for firms of their size. . . . DIB firms in this group are likely struggling either to have sufficient cybersecurity professionals or to maintain a full suite of [cybersecurity tools], and they likely cannot have both at the same time."[118]

"Small firms, including those in the DIB, often lack the necessary resources—including adequate budget, dedicated information technology (IT) staff, and/or experienced personnel—to procure and maintain a robust cyber defense, particularly against sophisticated nation-state adversaries."

The situation is exacerbated by the fact that small businesses face enormous market pressure.[119] Such pressure is particularly acute in the DIB, where the number of SMEs has dropped by 40 percent in the past decade.[120] Responding to market pressure, small businesses compete by maintaining a laser-focus on maximizing revenue (e.g., by minimizing costs and reducing time to market). In this environment, cybersecurity investments, which generally do not generate revenue, are not a top business priority.[121]

It is worth underscoring that developing and operating an effective cybersecurity program requires expertise that

112 Exec. Order 14017, 86 Fed. Reg. 11849 (February 24, 2021).

113 Lawrence A. Gordon, Martin P. Loeb et al., "Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms," *Journal of Information Security* 9, No. 2, April 2018, https://www.scirp.org/journal/paperinformation.aspx?paperid=82419.

114 "Many [SMBs] believe that they are too small to get targeted by hackers," according to a Software Testing Help survey. See "Top 10 MDR Services: Managed Detection and Response Solutions," Software Testing Help, Updated November 1, 2021, https://www.softwaretestinghelp.com/mdr-services/. In a separate survey of 500 senior decision makers at SMBs, two out of three respondents believed a cyber intrusion was unlikely, although two out of three SMBs experienced an intrusion in the past year; see "Cyber Mindset Exposed: Keeper Unveils Its 2019 SMB Cyberthreat Study," *Keeper (*blog), Keeper Security, July 24, 2019, https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/. Some SMBs incorrectly believe that "digital hackers are inclined to go after enterprises or large targets only." See "Security Poverty Line: What It Is and What You Can Do About It," *Sentinel Intrusion Prevention Systems,* August 20, 2021, https://sentinelips.com/2021/08/20/security-poverty-line/.

115 Daniel Gonzales et al., *Unclassified and Secure: A Defense Industrial Base Cyber Protection Program for Unclassified Defense Networks*, Rand Corporation, 2020, 36, https://www.rand.org/pubs/research_reports/RR4227.html.

116 "Security Poverty Line"; see also "The Security Bottom Line Report," *Cisco Cybersecurity Series*, October 2019, 4, https://www.cisco.com/c/dam/global/en_uk/products/pdfs/cybersecurityseries_bottomline.pdf; Wendy Nather, head of Advisory Chief Information Security Officers (CISOs) at Cisco, coined the term security poverty line.

117 "The Security Bottom Line Report," 6.

118 Gonzales et al., *Unclassified and Secure*, 36.

119 *Hearing to Receive Testimony on the Cybersecurity of the Defense Industrial Base* (testimony of Salazar).

120 Id. Moreover, one in every seven small businesses in the DIB does not expect to return to prepandemic profitability. See Lamar Johnson, "DOD Could Do More to Help Small Businesses with CMMC Implementation, Compliance," *MeriTalk*, May 19, 2021, https://www.meritalk.com/articles/dod-could-do-more-to-help-small-businesses-with-cmmc-implementation-compliance/.

121 In a 2019 SMB cyberthreat survey, 9 percent of senior decision makers ranked cybersecurity as a top business priority; 18 percent ranked it as their lowest. See "Cyber Mindset Exposed."

most companies simply do not have.[122] In a recent survey of SME decision makers, 25 percent of respondents said they did not know where to start with cybersecurity.[123] As the foregoing implies, no single authoritative source exists for small business cybersecurity.[124] To be sure, a patchwork quilt of government, private sector, and nonprofit organizations offers small business cybersecurity resources for free or at a low cost.[125] Unfortunately, many of these resources offer guidance that is too general to be implemented,[126] or too technical to be of practical use to small businesses absent considerable IT expertise.[127] Some organizations offer free cybersecurity assessments to SMEs, but they generally do not provide a full architecture and often offer little direction as to how SMEs can improve their assessed security posture in a cost-effective manner (i.e., without purchasing expensive cybersecurity tools and services). Available cybersecurity offerings are largely fragmented,[128] with a notable lack of affordable, integrated cybersecurity offerings for SMEs.

A cybersecurity resilient architecture that will effectively support SMEs[129] and academia[130] engaged in developing and operating emerging and advanced technologies ("critical SMEs/academia") would have three key elements: a zero-trust architecture; a threat-hunting capability; and expert personnel to maintain the zero-trust architecture, to engage in threat hunting, and to undertake any necessary remediation.

122 SMEs cannot easily/cost-effectively acquire such expertise, particularly given the global shortage of skilled cybersecurity professionals, now estimated to stand at 2.72 million people. (ISC)² Cybersecurity Workforce Study, "A Resilient Cybersecurity Profession Charts the Path Forward," 2021, https://www.isc2.org/-/media/F829F79ADBDC4F6391432B7D122DA32E.ashx; and Nasrin Rezai, "How Can We Narrow the Talent Shortage in Cybersecurity," *Dark Reading* (cybersecurity news portal), October 25, 2021, https://www.darkreading.com/careers-and-people/how-we-can-narrow-the-talent-shortage-in-cybersecurity. Rezai, Verizon's chief information security officer, notes a common refrain in the field: "There just isn't enough talent."

123 "Cyber Mindset Exposed."

124 "The Security Bottom Line Report," 10.

125 For examples of cybersecurity resources and tools available for small businesses, see CISA, "Cyber Essentials Toolkits," https://www.cisa.gov/publication/cyber-essentials-toolkits; "GCA Cybersecurity Toolkit for Small Business," Global Cyber Alliance (website), https://www.globalcyberalliance.org/gca-cybersecurity-toolkit-for-small-business/; "NSA's Top Ten Cybersecurity Mitigation Strategies," NSA/Central Security Service, March 5, 2018, https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf; FCC Cybersecurity Hub, http://www.fcc.gov/cyberforsmallbiz; "CIS Critical Security Controls," Center for Internet Security, https://www.cisecurity.org/controls/cis-controls-faq/; "Stay Safe Online," National Cyber Security Alliance, https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/; and Mastercard Trust Center, https://www.mastercard.us/en-us/business/overview/safety-and-security/cyber-security.html. cf., Project Xander, a University of Texas San Antonio, National Security Collaboration Center initiative focused on building cyber resilience within faith-based and nonprofit organizations by promoting partnerships to advance community cyber security maturity models.

126 For general cybersecurity tips for small businesses including firewall security and security while employees work from home, see "Cybersecurity for Small Business," FCC, https://www.fcc.gov/general/cybersecurity-small-business.

127 For descriptions of how SMBs can enable domain-based message authentication, reporting, and conformance (DMARC) to prevent email spoofing, for example, see Jen McPhillips, "Preventing Spoofing with DMARC," https://help.coalitioninc.com/en/articles/3281159-preventing-spoofing-with-dmarc.

128 Ed Amoroso and Katie Teitler, *Tag Cyber's Security Annual: Market Outlook and Industry Insights* (Sparta, New Jersey: Tag Cyber LLC, 2021 Edition), 7-13, https://www.tag-cyber.com/downloads/2021_TAG-Cyber_Annual.pdf. The report identifies fifty-four areas of focus for CISO's developing enterprise security programs, and organizes the areas in a "periodic table of security." See also the top fifteen security technologies being used by survey respondents, how to connect all of that information, and conducting a cybersecurity audit before making decisions and budgeting in "The Security Bottom Line Report," 8, 10.

129 For the purposes of this paper, the abbreviation SME refers to firms with fewer than five hundred US-based employees (consistent with the US International Trade Commission definition referenced below). Congress can, of course, choose to define SMEs differently. While there is no universally accepted definition of SME, the term is widely understood to refer to a business that maintains revenue, assets, and/or a number of employees below a certain threshold. See US International Trade Commission (ITC), "Small and Medium Sized Enterprises: Overview of Participation in US Exports," January 2010, 1-2, https://www.usitc.gov/publications/332/pub4125.pdf; and Daniel Liberto, "Small and Mid-size Enterprise," Investopedia, https://www.investopedia.com/terms/s/smallandmidsizeenterprises.asp. Some useful guideposts regarding the definition of SMEs:
(a) The ITC has previously defined SMEs as firms with "fewer than five hundred US-based employees." See US ITC, Investigation No. 332-510, Publication 4189, "Small and Medium-Sized Enterprises: Characteristics and Performance," November 2010, xi, https://www.usitc.gov/publications/332/pub4189.pdf.
(b) Pursuant to the Small Business Act (15 U.S.C. § 632, as amended), the Small Business Administration (SBA) has promulgated detailed standards for determining whether a business is "small" (but not "medium"). See "Small Business Size Regulation," 13 CFR Part 121. The SBA generally uses average annual receipts and average number of employees to determine the size of a business, with small businesses ranging from $1 million to $41.5 million in revenues and anywhere from one hundred to 1,500 employees, depending on the industry. While size standards vary by industry, "[m]ost manufacturing companies with five hundred employees or fewer, and most nonmanufacturing businesses with average annual receipts under $7.5 million, will qualify as a small business." US Small Business Administration, "Basic Requirements," https://www.sba.gov/federal-contracting/contracting-guide/basic-requirements.
(c) The Internal Revenue Service generally relies on the "small business" definitions specified in individual tax laws, e.g., the Affordable Care Act, and by the SBA. Notably, the revenue service's "Small Business and Self-Employed Tax Center" is geared toward "small businesses with assets under $10 million." See IRS, "Small Business and Self-Employed Tax Center," https://www.irs.gov/businesses/small-businesses-self-employed.
(d) For research purposes, Gartner Inc. defines small businesses as organizations with fewer than one hundred employees and less than $50 million in annual revenue, and midsize businesses as organizations with one hundred to 999 employees and between $50 million and $1 billion in revenue. See Gartner Glossary, "Small and Midsize Business (SMB)," Gartner, https:www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses.
(e) Ohio State University's National Center for the Middle Market defines "the middle market" as companies with annual revenue between $10 million and $1 billion. See National Center for the Middle Market, "Promoting Growth of the US Middle Market," https://www.middlemarketcenter.org/Media/2021%20General%20Info%20Sheet.pdf.

130 The term "academia" is used herein to refer to universities and other "institutions of higher education" (defined at 20 U.S.C. § 1001), as those terms are used in 35 U.S.C. § 201(i).

> "A cybersecurity resilient architecture that will effectively support SMEs and academia engaged in developing and operating emerging and advanced technologies . . . would have three key elements: a zero-trust architecture; a threat-hunting capability; and expert personnel"

To effectuate such a cybersecurity resilient architecture for critical SMEs/academia (which cannot generate such capabilities on their own) requires: zero-trust architecture implemented for critical SMEs/academia by a cybersecurity provider; cloud-delivered security (i.e., security as a service), leveraging artificial intelligence/machine learning; operation by expert providers, working in conjunction with critical SMEs/academia; and federal government funding through transferrable "cybersecurity investment tax credits." Each of these elements is more fully described below.

A. Zero-trust Architectures

The recent executive order on cybersecurity for the federal government identifies zero-trust architectures (ZTAs) as a key component in establishing such security.[131] The key elements of a zero-trust architecture have been usefully summarized as follows:

> The core principles behind ZT are: 1) universal authentication of all users, devices, and services; 2) access segmentation, allowing no single entity access to more than a small portion of the organization's resources; 3) minimal trust authorization, keeping access to resources only to those entities that "need-to-know" and can be trusted; 4) encryption everywhere to protect information in flight and at rest, whether inside or outside the organization's networks; and 5) continuous monitoring and adjustment to detect issues early and adjust access accordingly.[132]

Zero-trust security is an alternative to the traditional "perimeter security" model.[133] The traditional model automatically trusted users and end points within the organization's perimeter.[134] In contrast, the zero-trust model is a "deny by default" security framework. Zero-trust frameworks "requir[e] all users, whether in[side] or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data."[135]

As the NSA has stated, "The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity."[136] The zero-trust model has been further described by the NSA as:

> embed[ding] comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to

131 Exec. Order 14028, 86 Fed. Reg. 26633, Sections 3 and 10(k) (May 12, 2021), https://www.federalregister.gov/d/2021-10460/p-33 and https://www.federalregister.gov/d/2021-10460/p-154, respectively. ZTAs are based on the "never trust, always verify" principle and involve controlling access to the "protect surface" which is made up of the "network's most critical and valuable data, assets, applications, and services—DAAS, for short. . . . Because it contains only what's most critical to an organization's operations, the protect surface is orders of magnitude smaller than the attack surface, and it is always knowable." See also "What Is a Zero Trust Network," Palo Alto Networks (website), https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

132 K. D. Uttecht, "Zero Trust (ZT) Concepts for Federal Government Architectures," Lincoln Laboratory, Massachusetts Institute of Technology, Technical Report 1253, July 30, 2020, https://apps.dtic.mil/sti/pdfs/AD1106904.pdf. The development and implementation of mechanisms for authentication and continuous monitoring raise important privacy and security concerns. Properly implemented, a ZTA will preserve privacy and civil liberties while meeting the requirements for universal authentication and continuous monitoring.

133 John Kindervag, "Build Security into Your Network's DNA: The Zero Trust Network Architecture," Forrester Research, November 5, 2010.

134 Jeannie Warner, "What Is Zero Trust Security?," CrowdStrike, May 6, 2021. The term "zero trust" was coined by Forrester Research analyst and thought leader John Kindervag, and follows the motto, "never trust, always verify." His ground-breaking view was based on the assumption that risk is an inherent factor both inside and outside the network.

135 Warner, "What is Zero Trust Security?"; and Technologent, "Key Components of the Zero Trust Security Model," https://blog.technologent.com/key-components-zero-trust-security-model. ("Every user and device attempting to access network resources must be verified, whether inside or outside the network perimeter. . . . Use multifactor authentication to prevent network access with stolen passwords. Strictly enforce access controls. Learn who users are, what devices and applications they use, and how they connect to the network so that unusual behavior can be detected.")

136 National Security Agency, "Embracing a Zero Trust Security Model," NSA Cybersecurity Information, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

VULNERABILITY OF SMALL AND MEDIUM ENTERPRISES

"Smaller companies or biotech start-ups may not view themselves as cyber targets, or if they do, they may not have the resources to address the risks adequately," according to the National Academies of Sciences, Engineering, and Medicine. "Small companies and start-ups are generally more vulnerable to cyber intrusions relative to large organizations. Even if they have skilled information technology departments, such organizations typically have neither the budget nor the security focus to fend off attackers, nor do they have much actual experience in this arena. . . . They may not employ state-of-the art defenses, such as multifactor authentication, and users who have not been properly educated on these matters are more likely to fall for phishing attacks and the like. In addition, most application programmers have little, if any, education in how to write secure code, opening the door to even low-end attackers."[1]

1 National Academies of Sciences, Engineering, and Medicine, *Safeguarding the Bioeconomy* (Washington, DC: The National Academies Press, 2020), 306, https://doi.org/10.17226/25525.

resources based on the combination of several contextual factors.[137]

With its "focus on protecting critical assets," zero trust provides for the greatest protection to the most important assets and data.

B. Cloud-based Security

As is generally understood, the "term 'cloud' refers to the technologies that allow people to access computing resources from anywhere through the Internet."[138] More technically, the National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[139] These capabilities, as available through the use of the cloud, allow security to be provided as a service by expert cloud service providers.[140]

As the foregoing indicates, the use of cloud computing for SMEs and academia allows the benefits of scaling and optimization of resources to be available to entities that could not achieve such results acting on their own. A service provider utilizing the cloud can engage multiple experts in a way that a single enterprise cannot. As the National Security Telecommunications Advisory Committee has stated, many smaller and midsized "enterprises will [need to] rely upon ICT providers to better assure their security . . . [including] cloud service . . . [which] can provide multiple network security functions, including firewalls, intrusion prevention systems, secure web and email gateways, remote access tools, routing, and Wide Area Networking (WAN) connectivity. The value of this type of hardware or service is that it protects businesses from security threats

> "the use of cloud computing for Small and Medium Enterprises and academia allows the benefits of scaling and optimization of resources to be available to entities that could not achieve such results acting on their own"

137 NSA, "Embracing a Zero Trust Security Model."

138 Lloyd's and AIR Worldwide, *Cloud Down: Impacts on the US Economy,* Emerging Risk Report 2018: Technology, 2018, https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2018/cloud-down/aircyberlloydspublic2018final.pdf.

139 Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Department of Commerce, Special Publication 800-145, September 2011, 2, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

140 Amazon Web Services, Microsoft Azure, and Google Cloud are the so-called "hyperscale" US cloud providers, as noted by Peter Bendor-Samuel, "Hyperscale Cloud Providers Shaping the Platform Marketplace," *Forbes*, March 2, 2020, https://www.forbes.com/sites/peterbendorsamuel/2020/03/02/hyperscale-cloud-providers-shaping-the-platform-marketplace/?sh=47a411a1103d.

using a simplified approach, requiring less individual expertise across multiple systems."[141]

It is essential that critical SMEs/Academia rely on trusted vendors when migrating to the cloud. As an important corollary, critical SMEs/Academia and cybersecurity providers receiving the tax credits described below, would be prohibited from relying on technology providers that the US government does not trust, including Chinese cloud service providers such as Alibaba, Tencent, and Huawei, each of which has close links with the Chinese government.[142] Cybersecurity and technology expert James Lewis, who is senior vice president at the Center for Strategic and International Studies (CSIS), recently put it this way: "No one in their right mind should use a Chinese cloud service . . . it's like inviting the Ministry of State Security or the [People's Liberation Army] to listen in."[143]

Cloud security includes "the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure against both external and internal cyber threats."[144] Accelerating the migration to cloud puts a premium on cloud security, not the least because cloud computing itself can be a source of supply chain risk,[145] and because of the "systemic risk associated with a centralized approach."[146] Accordingly, cloud providers for critical SMEs/academia need to have appropriate controls, and the availability of multiple certified providers, as described below, will add to diversity, thereby reducing centralization risks.

Today's leading cloud providers often follow a "shared responsibility model" of security,[147] in which the cloud provider is responsible for the security *of* the cloud,[148] and the customer is responsible for security *in* the cloud.[149] For this reason, in such situations, "[e]ffective cloud security depends on consumers knowing and meeting all [of] their security responsibilities."[150] However, as explained above, critical SMEs/Academia generally cannot meet such requirements. Rather, the fundamental point is for security to be provided as a service precisely because of such limitations; critical SMEs/Academia will need expert capabilities provided by cybersecurity service providers utilizing the cloud. As one example, critical SMEs/Academia generally will not have the resources or personnel to utilize AI to bolster their cybersecurity. AI is a key component of effective cybersecurity because it is essential to the automation of key steps of the threat prevention, detection, and response process. In fact, AI is a critical component of continuous monitoring, which, as noted above, is a necessary element of a zero-trust architecture. Expert cybersecurity service providers can offer SMEs the benefits of AI-driven cybersecurity. Likewise, maintaining the necessary authentication,

141 National Security Telecommunications Advisory Committee, "NSTAC Report to the President on Communications Resiliency," May 6, 2021, 12, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency.pdf.

142 Such an approach would be consistent with the broad national security goals animating the "clean cloud" program. Michael Garcia, "The Future of 'Clean Cloud,' " Guest Blog Post, *Net Politics*, Council on Foreign Relations, September 28, 2020, https://www.cfr.org/blog/future-clean-cloud. Announced on August 5, 2020, by then-Secretary of State Mike Pompeo, the "Clean Cloud" program was designed "to prevent US citizens' most sensitive personal information and our businesses' most valuable intellectual property . . . from being stored and processed on cloud-based systems accessible to our foreign adversaries through companies such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent." US Department of State, "The Clean Network," https://2017-2021.state.gov/the-clean-network/index.html. The proposed approach also would be consistent with the more-nuanced framework recently set forth to assess the challenges of Chinese-owned platforms operating in the United States; see Gary Corn et al., "Chinese Technology Platforms Operating in the United States: Assessing the Threat," Hoover Institution, February 11, 2021, https://www.hoover.org/sites/default/files/research/docs/chinesetechplatforms_webreadypdf.pdf.

143 Mercy Kuo, "'Clean Network' in the US-China Tech Race: Insights from James Andrew Lewis," *Diplomat*, March 1, 2021, https://thediplomat.com/2021/03/clean-network-in-the-us-china-tech-race/. Lewis also directs the CSIS Strategic Technologies Program.

144 Christopher J. Alberts, "A Prototype Set of Cloud Adoption Risk Factors," Carnegie Mellon University Software Engineering Institute, April 2021, 26, https://resources.sei.cmu.edu/asset_files/WhitePaper/2021_019_001_740892.pdf.

145 Trey Herr, "Four Myths About the Cloud: The Geopolitics of Cloud Computing," Atlantic Council, August 31, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing. Herr says: "Cloud computing ties corporate decision-making driven by business risk even more closely to national security risk as a single provider's supply chain decisions and internal security policies can impact millions of customers." For example, teams of hackers connected to the Chinese Ministry of State Security infiltrated US cloud service providers in a global cyberespionage campaign known as "Cloud Hopper." The attackers "hopped" into client networks and stole US government and corporate secrets. See Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's Failed Fight against China's 'Cloud Hopper' Hackers," Reuters, June 16, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

146 Tim Maurer and Garrett Hinck, "Cloud Security: A Primer for Policymakers," Carnegie Endowment for International Peace, August 2020, 2, https://carnegieendowment.org/files/Maurer_Hinck_Cloud_Security-V3.pdf. This has been dubbed the "cloud concentration risk," referring to the idea that "the consolidation of multiple organizations within one cloud service provider (CSP) presents a more attractive target for cybercriminals." Ron Shevlin, "Banks' False Sense of Cybersecurity Will Be Shattered By Cloud Computing," *Forbes*, August 17, 2020, https://www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/?sh=118ea44a24ae.

147 Alberts, "A Prototype Set of Cloud Adoption Risk Factors," 26.

148 "The level of oversight that an organization must perform to confirm the [cloud service provider's] security controls depends on the contracting provisions in place for information sharing." Alberts, "A Prototype Set of Cloud Adoption Risk Factors," 26; and see Randy Armknecht, "Cloud Oversight in Financial Services: Understanding Responsibility and Control," Protiviti (business consulting blog), https://blog.protiviti.com/2020/06/25/cloud-oversight-in-financial-services-understanding-responsibility-and-control/.

149 Amazon Web Services, "Shared Responsibility Model," https://aws.amazon.com/compliance/shared-responsibility-model/; and Microsoft, "Shared Responsibility for Cloud Computing," Version 2.0, October 2019, https://azure.microsoft.com/mediahandler/files/resourcefiles/shared-responsibility-for-cloud-computing/Shared%20Responsibility%20for%20Cloud%20Computing-2019-10-25.pdf.

150 Timothy Morrow et al., *Cloud Security Best Practices Derived from Mission Thread Analysis*, Technical Report, Carnegie Mellon University Software Engineering Institute, July 2019, Updated September 2021, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2021_005_001_551472.pdf.

segmentation, authorization, and encryption are all tasks requiring a high level of expertise.

C. Expert Capabilities

In addition to the expertise required for the operation of the cloud itself, expert providers are necessary to engage in cyber-threat hunting and to support any required remediation.

As one description provides:

> "Threat hunting is highly complementary to the standard process of incident detection, response, and remediation. As security technologies analyze the raw data to generate alerts, threat hunting is working in parallel—using queries and automation—to extract hunting leads out of the same data. . . . Hunting leads are then analyzed by human threat hunters, who are skilled in identifying the signs of adversary activity, which can then be managed through the same pipeline."[151]

Effective threat hunting requires a "three-pronged approach . . . [of] vast data and powerful analytics . . . [and] [i]ntrusion analysts . . . [with] expertise to identify sophisticated targeted attacks."[152]

Threat hunting can also utilize, and be complemented by the use of, active defense[153]—particularly deception[154]—within the network. Within that context, "[t]he active deception category of active defense systems can provide significant value within most organizations. The basic idea behind these systems is to increase the cost for an attacker to successfully exfiltrate sensitive data."[155] For private entities, it is important to underscore that active defense is limited to actions on the entity's own networks;[156] "hacking back" outside those networks is an activity reserved to the federal government.

Cyber-threat hunting is a necessary element of effective cybersecurity resilience because even a zero-trust architecture will not prevent all successful intrusions into a network. The federal executive order on cybersecurity calls for "active cyber hunting" and requires a report on "conduct[ing] threat-hunting activities on [federal] networks without prior authorization from agencies . . . [including] recommend[ed] procedures to ensure that mission-critical systems are not disrupted . . . and the range of techniques that can be used."[157] A comparable approach would support cybersecurity for critical SMEs/Academia.

"a feasible funding model . . . for SMEs and academia . . . that generally have limited funds [would be] [t]he establishment of transferable cybersecurity tax incentive credits"

D. Financial Resources

Assuming the availability of a zero-trust architecture with threat-hunting capability from expert providers, a feasible funding model has to be established for SMEs and academia, entities that generally have limited funds. The establishment of transferable cybersecurity tax incentive credits would resolve this issue.

Congress regularly relies on investment tax credits and other so-called tax expenditures to spur desired investment in specified industrial sectors.[158] The federal government incentivizes R&D investment across all sectors through the federal R&D credit that is available to eligible companies in

151 Scott Taschler, "What Is Cyber Threat Hunting?," CrowdStrike 2021 Threat Hunting Report, February 18, 2021, https://www.crowdstrike.com/cybersecurity-101/threat-hunting/#:~:text=Threat%20hunting%20is%20the%20practice,your%20initial%20endpoint%20security%20defenses.

152 Taschler, "What Is Cyber Threat Hunting?"

153 Active Defense Task Force, George Washington University (GWU) Center for Cyber and Homeland Security, "Into the Gray Zone: The Private Sector and Active Defense Against Cyber Threats," October 2016, 9-15, https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf. The center is no longer located at GWU.

154 Deborah L. Schuh, MITRE Center for Technology and National Security, *The Cyberspace Advantage: Inviting Them In! How Cyber Deception Enables Better Resilience*, https://www.mitre.org/sites/default/files/publications/pr-19-3726-cyberspace-advantage-ctns.pdf.

155 Josh Johnson, *Implementing Active Defense Systems on Private Networks,* SANS Institute, 2021, 3, https://sansorg.egnyte.com/dl/xTL7hD0RKB.

156 GWU, "Into the Gray Zone," 17, https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf.

157 Exec. Order 14028, sections 7(b) and 7(i), https://www.federalregister.gov/d/2021-10460/p-123.

158 The government forgoes an estimated $1.5 trillion in revenue annually through income-related tax expenditures. "Tax Expenditures—The $1.5 Trillion Elephant in the (Budget) Room," *Bloomberg Tax*, September 7, 2021, https://news.bloomberglaw.com/daily-tax-report/tax-expenditures-the-1-5-trillion-elephant-in-the-budget-room.

ACADEMIA-GOVERNMENT COLLABORATION

1) Larger state universities may have cybersecurity options not generally available to most of academia. For example, in Texas, the Texas A&M University System (TAMUS) provides security operations center services to TAMUS' campuses across the state. It has also partnered with the Texas Department of Emergency Management to offer monitoring and incident response services to other SMEs in the state including county and city government as well as local utilities. TAMUS has been recognized by the Defense Security Service for excellence in counterintelligence, works closely with other federal and state authorities, and is leveraging its experience to expand its efforts to provide managed cloud services and threat hunting as well as security consulting in the areas of new system design, business continuity, disaster recovery planning and securing infrastructure on its network and its extended enterprise network.[1] If such arrangements otherwise meet the requirements described in this report, they should qualify for the transferable investment tax credits described below for the portion of the effort devoted to cybersecurity for qualified activities.

2) As part of the federal government's Manufacturing USA program,[2] the Department of Energy established the Cybersecurity Manufacturing Innovation Institute (CyManII) in 2020.[3] CyManII, led by the University of Texas-San Antonio,[4] will receive federal funding of $70 million,[5] and, according to its director, is intended to "get to the holy grail of cybersecurity, which is to design systems of systems that are secure by design."[6]

1 Security Operations Center—Organization & Mission Briefing, Texas A&M University, accessed November 18, 2021. Reviewed by author.

2 Manufacturing USA, accessed December 17, 2021, https://www.manufacturingusa.com/

3 Congressional Research Service, Manufacturing USA: Advanced Manufacturing Institutes and Network, 7, March 3, 2021, https://crsreports.congress.gov/product/pdf/R/R46703

4 "Department of Energy Picks UTSA for $111 Million Cybersecurity Institute," Security, May 29, 2020, https://www.securitymagazine.com/articles/92481-department-of-energy-picks-usta-for-111-million-cybersecurity-institute

5 Id. at p. 8.

6 Brett Brune, Meet CyManII, "Uncle Sam's 2020 nod to the urgency of cybersecurity," *SME,* January 21, 2021, https://www.sme.org/technologies/articles/2021/february/meet-cymanii-uncle-sams-2020-nod-to-the-urgency-of-cybersecurity/

connection with the development of new products, manufacturing processes, and software.[159] Specific sectors likewise receive support. In the energy sector, for example, the energy investment credit (EIC) provides up to 30 percent credit for specified renewable energy investments including qualified solar,[160] geothermal,[161] and wind energy property; [162] the oil and gas industry benefits from tax expenditures (and other tax provisions such as immediate expensing and bonus depreciation) that "reduce the after-tax cost of investing in oil and gas exploration and production, encouraging additional investment in [the oil and gas] sector relative to other economic sectors,"[163] and the tax code provides investment tax credits for "clean coal facilities producing electricity and for industrial gasification combined cycle projects."[164]

Investment in cybersecurity resilient architectures through cybersecurity investment tax credits should be incentivized in the same manner by Congress. To be eligible for a cybersecurity investment tax credit, SMEs or academia must be undertaking qualifying activities in emerging and advanced technologies as designated by Congress.

159 Alex Muresianu, "Reviewing the Federal Tax Treatment of Research and Development Expenses," Tax Foundation, April 13, 2021, https://taxfoundation.org/research-and-development-tax/.

160 Energy Credit, 26 I.R.C. § 48, https://www.govinfo.gov/content/pkg/USCODE-2011-title26/pdf/USCODE-2011-title26-subtitleA-chap1-subchapA-partIV-subpartE-sec48.pdf; see also Department of Energy, Office of Energy Efficiency and Renewable Energy, "Guide to the Federal Investment Tax Credit for Commercial Solar Photovoltaics," https://www.energy.gov/sites/default/files/2021/02/f82/Guide%20to%20the%20Federal%20Investment%20Tax%20Credit%20for%20Commercial%20Solar%20PV%20-%202021.pdf, (which explains that a taxpayer eligible for the commercial ITC for a solar photovoltaic system that is placed in service typically can also take advantage of accelerated depreciation to reduce the overall cost of its installation).

161 Energy Credit, 26 I.R.C. § 48.

162 US Department of Treasury, FY 2022 Tax Expenditure Report, 6, https://home.treasury.gov/system/files/131/Tax-Expenditures-FY2022.pdf.

163 Congressional Research Service, "Oil and Gas Tax Preferences," In Focus (brief), IF11528, Version 3, Updated April 16, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11528#:~:text=Several%20features%20of%20the%20income,of%20oil%20and%20gas%20companies.&text=Tax%20preferences%20for%20oil%20and%20gas%20reduce%20the%20after%2Dtax,relative%20to%20other%20economic%20sectors.

164 US Department of Treasury, FY 2022 Tax Expenditure Report, 6.

SHORTAGE OF CYBER-THREAT HUNTERS

Human capital is essential to cybersecurity, but demand is outpacing supply.[1] Today, we face a global shortage of the skilled cybersecurity professionals essential to effective cybersecurity (including threat hunting) for critical SMEs. Leveraging automation, machine learning, and AI for repetitive, time-consuming, and data-intensive tasks will support and enhance cybersecurity, while freeing skilled cybersecurity professionals to focus on higher-value tasks.

1 (ISC)[2] Cybersecurity Workforce Study, "A Resilient Cybersecurity Profession Charts the Path Forward"; and NSA, "Embracing a Zero Trust Security Model."

Illustratively, such technologies might include an identified list such as artificial intelligence, quantum computing, biotechnology, robotics, additive manufacturing, and climate change mitigation or adaptation, or alternatively refer to those identified as "critical" in existing statutes such as the Foreign Investment Risk Review and Modernization Act of 2018,[165] and its implementing regulations.[166] "Qualifying activities" should also require the entity's business (research, in the case of academia) to be substantially focused on a designated technology or technologies (e.g., at least 50 percent) or, alternatively, for activities for that technology effort to be greater than a threshold amount set by Congress.

If the qualifying requirements are met, the entity would be eligible to receive a cybersecurity investment tax credit. The amount of the credit could be equal to the cost of the cybersecurity resilient architecture charged by the cybersecurity provider—or, if Congress determined, a multiple (perhaps 1.5 times) to further incentivize the use of cybersecurity resilient architectures to support emerging and advanced technologies. Since many SMEs and academia may not have use for tax credits, such credits would be transferable to the cybersecurity provider, with the transfer being taken as payment for the cybersecurity service.

To avoid pricing manipulation, the cybersecurity provider would have to certify that the pricing model utilized for the SME/academia was substantially equivalent to that used in pricing for other comparable customers.

Cybersecurity investment tax credits would be transferable only to providers certified to implement a zero-trust architecture and effective threat-hunting program equivalent to what is required of the federal government under the executive order on cybersecurity. Such providers would be required to attain a level of capability more effective than the top tier of the DOD's Cybersecurity Maturity Model Certification (CMMC) 2.0 program.[167] Certification could be accomplished by the federal government—most likely by CISA—or through the use of a private-sector capability such as a nonprofit along the lines of the Underwriters Laboratory or potentially by providing additional authorities to an Information Sharing and Analysis Organization. Importantly, by concentrating on protecting a smaller set of critical organizations rather than requiring thousands of enterprises to self-certify, this approach avoids many of the issues that have plagued the CMMC effort. Properly structured, the proposed approach, funded through the investment tax credit, would bring "best-in-class" technology and services to critical SMEs/academia.[168]

165 50 U.S.C. § 4817 (2018).

166 31 C.F.R. § 800.215, (defining "critical technologies" to include, inter alia, emerging and foundational technologies controlled under Section 1758 of the Export Control Reform Act of 2018, 50 U.S.C. § 4817; defense articles on the US Munitions List set forth in the International Traffic in Arms Regulations, 22 C.F.R. parts 120-130; and items on the Commerce Control List set forth in the Export Administration Regulations). "Critical technologies" are defined similarly in the Endless Frontier Act (S. 1260), which the Senate passed in June 2021 and now awaits action in the House of Representatives, https://www.congress.gov/bill/117th-congress/senate-bill/1260?q=%7B%22search%22%3A%5B%22Endless+Frontier%22%5D%7D&r=1&s=2m.

167 CMMC 2.0's top tier is "Compliance Level 3" and will be based on a subset of NIST SP 800-172 requirements, which themselves are intended to supplement the security requirements found in NIST SP 800-171. See "CMMC Model," Office of the Under Secretary of Defense, Acquisition & Sustainment (website), https://www.acq.osd.mil/cmmc/model.html; and Ron Ross et al., NIST Special Publication 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, February 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf.

168 The model described above could be expanded. One area that deserves review is the nonprofit arena. Nation-state actors, like the PRC, are beginning to more actively target these vulnerable small enterprises, many of which have valuable information including personal identity information. NGOs and think tanks were the second-most targeted sector by cybercriminals, accounting for 16 percent of all notifications of nation-state attacks against organizational domains as detected by Microsoft. See *Microsoft Digital Defense Report*, Microsoft, October 2021, 61, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi?id=101738. According to a recent guide for the nonprofit sector, up to 70 percent of charity networks lack a comprehensive vulnerability assessment to determine risk. See tca SynerTech, "2021 Cybersecurity Guide for Nonprofit Organizations," https://www.tcasynertech.com/2021-cybersecurity-guide-for-nonprofit-organizations/. As one approach, the University of Texas at San Antonio, in conjunction with MITRE Corporation acting as an expert provider, is now offering vulnerability assessments to San Antonio community nonprofits with the intent of scaling this type of service with other state university systems nationwide.

IV. Conclusion

Maintaining the United States' innovative advantage is crucial to both national and economic security. Expert-provided cybersecurity resilient architectures are critical elements in securing such advantage. The administration and the Congress should work together, along with the private-sector cybersecurity expert community, to establish and implement such capabilities.

About the Authors

Franklin D. Kramer is a distinguished fellow at and serves on the board of the Atlantic Council. He is a former assistant secretary of defense for international security affairs.

Melanie J. Teplinsky is an adjunct professor at American University, Washington College of Law, where she is a senior fellow in the Technology, Law and Security Program. She served (pre-IPO) on the advisory board for CrowdStrike Inc. and previously practiced technology law at Steptoe & Johnson LLP.

Robert J. Butler is the co-founder and managing director of Cyber Strategies LLC, served as the first deputy assistant secretary of defense for space and cyber policy, and has acted as an adviser to the Texas A&M University and University of Texas systems.

Mr. Kramer and Ms. Teplinsky are co-authors of "Cybersecurity and Tailored Deterrence," and Mr. Kramer and Mr. Butler are co-authors of *Cybersecurity: Changing the Model*.

Atlantic Council

Board of Directors

Atlantic Council

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