Cybersecurity for Innovative Small and Medium Enterprises and Academia

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

**Executive Summary**  
1

I. **The Challenge**  
2

II. **The Importance of Protecting SMEs and Academia**  
7  
   A. SMEs  
   7  
   B. Academia  
   8

III. **Meeting the Cybersecurity Challenge for SMEs and Academia**  
11  
   A. Zero-trust Architectures  
   14  
   B. Cloud-based Security  
   15  
   C. Expert Capabilities  
   17  
   D. Financial Resources  
   17

IV. **Conclusion**  
20

**About the Authors**  
21
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 base³ 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. 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, "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.”

---

⁷ “A Conversation with Christopher Wray.”
and its state-driven industrial policies, 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.”\(^9\) 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 Security

---

9 Industrial policies of particular note:
(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.


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

---
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

---


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=201905031453353529. (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.”


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.”)


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


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.\textsuperscript{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),\textsuperscript{33} focused efforts to staunch the Chinese cybersecurity 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.\textsuperscript{34} The hacking group had been active since at least 2013,\textsuperscript{35} and historically had shown interest in targets “connected to South China sea issues.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{38}

The impact of cyber espionage, which “accounts for a majority . . . of IP theft,”\textsuperscript{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 cyberspionage constitutes the “greatest transfer of wealth in history.”\textsuperscript{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.”\textsuperscript{41} Other estimates place US losses “between $20 billion and $30 billion annually from Chinese cyber espionage for decades.”\textsuperscript{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.\textsuperscript{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


\textsuperscript{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”).


\textsuperscript{37} Mandiant Inc. (formerly FireEye), “Suspected Chinese Cyber Espionage Group.”


\textsuperscript{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/FY20-INDUSTRIAL-CAPABILITIES-REPORT.PDF.

\textsuperscript{42} Lewis, “How Much Have the Chinese Actually Taken?”

\textsuperscript{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.”)
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.”

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. 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.”

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.”

---

1. Cybersecurity for Innovative Small and Medium Enterprises and Academia
II. The Importance of Protecting SMEs and Academia

A. SMEs

SMEs are significant generators of innovation across all US industry sectors. 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.” Similarly, small biotechnology companies “hold approximately 80 percent of the development pipeline for new medicines, diagnostics and other bio-based products.” Likewise, SMEs are essential “engines of innovation and vitality,” 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. 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. 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.”

Many of today’s most innovative companies began as SMEs. In the IT sector, these companies include household names such as Google, Facebook, Microsoft, Apple, Amazon, Oracle, Dell, and Cisco, as well as

“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.’”
as leading cybersecurity firms such as CrowdStrike, FireEye, Palo Alto Networks, and Tenable. 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.

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. Mitchell Energy revolutionized the energy sector in the late 1990s through the implementation of fracking, an efficient method of unlocking natural gas from shale; the business ultimately sold for $3.1 billion. 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. Tesla, founded in 2003 to develop an electric sports car, 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. 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.” 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. A host of familiar innovations—including cell phone technologies, the key filtration technology used in N95 respirators, the nicotine filtration technology used in N95 respirators, the nicotine


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/.


72 Zuckerman, “Breakthrough: The Accidental Discovery.”


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/.


78 The “resistive touch screen,” for example, was developed by Samuel Hurst at the University of Kentucky in 1971, while the “multicore processor” was 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.

Universities became “hotbeds of innovation” with the passage of the Bayh-Dole Act in 1980. 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, the act was “instrumental in encouraging universities to participate in technology transfer activities.” 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.

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. 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.  

---

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.”
81 Coumadin for treating blood clots, and Allegra for allergy relief—have their origins in university research.
82 Cochlear implants, Coumadin for treating blood clots, and Allegra for allergy relief—have their origins in university research.
83 ATLANTIC COUNCIL
84 Universities became “hotbeds of innovation” with the passage of the Bayh-Dole Act in 1980. 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, the act was “instrumental in encouraging universities to participate in technology transfer activities.” 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.

93 “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.
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.  

- 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.”

- 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. Stanford played a key role in the development of the nation’s high-tech hub in Silicon Valley. 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.”

- MIT researchers are responsible for technological advancements across a variety of fields over the past 150 years. 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. 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; and led groundbreaking energy research that eventually could lead to an emissions-free power plant.

- 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). Carnegie Mellon’s Center for Technology Transfer and Enterprise Creation fosters efforts to bring CMU research to market.

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


96 Trikha, “The Interdependency of Stanford and Silicon Valley.”


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_SSlgotege_.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).
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 combating 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.\textsuperscript{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.\textsuperscript{113} While many SMEs lack understanding and awareness of the cyber threats facing them,\textsuperscript{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.\textsuperscript{115} Many SMEs are below the “security poverty line,” a term coined to describe a lack of resources to implement the cybersecurity they need.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{118}

The situation is exacerbated by the fact that small businesses face enormous market pressure.\textsuperscript{119} Such pressure is particularly acute in the DIB, where the number of SMEs has dropped by 40 percent in the past decade.\textsuperscript{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.\textsuperscript{121}

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

---

\textsuperscript{118} Gonzales et al., Unclassified and Secure, 36.
\textsuperscript{119} Hearing to Receive Testimony on the Cybersecurity of the Defense Industrial Base (testimony of Salazar).
\textsuperscript{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/.
\textsuperscript{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. In a recent survey of SME decision makers, 25 percent of respondents said they did not know where to start with cybersecurity. As the foregoing implies, no single authoritative source exists for small business cybersecurity. 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. Unfortunately, many of these resources offer guidance that is too general to be implemented, or too technical to be of practical use to small businesses absent considerable IT expertise. 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, with a notable lack of affordable, integrated cybersecurity offerings for SMEs.

A cybersecurity resilient architecture that will effectively support SMEs and academia 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.

---


123 “Cyber Mindset Exposed.”


125 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 absent considerable IT expertise.


127 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/smallandsizemidenterprise.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.orgMEDIA/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).
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. The key elements of a zero-trust architecture have been useful 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.

Zero-trust security is an alternative to the traditional “perimeter security” model. The traditional model automatically trusted users and end points within the organization’s perimeter. In contrast, the zero-trust model is a “deny by default” security framework. Zero-trust frameworks “require[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.”

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.” 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.


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.”)

resources based on the combination of several contextual factors.\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{139}

These capabilities, as available through the use of the cloud, allow security to be provided as a service by expert cloud service providers.\textsuperscript{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.

\begin{footnotesize}
\textsuperscript{137} NSA, “Embracing a Zero Trust Security Model.”
\textsuperscript{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=47a41a1f103d.
\end{footnotesize}
Cybersecurity for Innovative Small and Medium Enterprises and Academia

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. 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.”

Cloud security includes “the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure against both external and internal cyber threats.” 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, and because of the “systemic risk associated with a centralized approach.” 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, in which the cloud provider is responsible for the security of the cloud, and the customer is responsible for security in the cloud. For this reason, in such situations, “[e]ffective cloud security depends on consumers knowing and meeting all [of] their security responsibilities.” 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, using a simplified approach, requiring less individual expertise across multiple systems.


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.”  

Effective threat hunting requires a “three-pronged approach . . . [of] vast data and powerful analytics . . . [and] intrusion analysts . . . [with] expertise to identify sophisticated targeted attacks.”

Threat hunting can also utilize, and be complemented by the use of, active defense—particularly deception—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.” For private entities, it is important to underscore that active defense is limited to actions on the entity’s own networks; “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.” A comparable approach would support cybersecurity for critical SMEs/Academia.

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. The federal government incentivizes R&D investment across all sectors through the federal R&D credit that is available to eligible companies in

---


152 Taschler, “What Is Cyber Threat Hunting?”


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

connection with the development of new products, manufacturing processes, and software.\textsuperscript{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,\textsuperscript{160} geothermal,\textsuperscript{161} and wind energy property;\textsuperscript{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.”\textsuperscript{163} and the tax code provides investment tax credits for “clean coal facilities producing electricity and for industrial gasification combined cycle projects.”\textsuperscript{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.
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, and its implementing regulations. “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 transferrable 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. 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.
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.
CHAIRMAN
**John F.W. Rogers

EXECUTIVE CHAIRMAN
EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*A. Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
John Bonsell
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Alan H. Fleischmann
*M. Michael Fisch
Jendayi E. Frazer
Meg Gentile
Thomas H. Glozer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Frank Haun
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Andrew Hove
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Yann Le Pallec
Deborah Lee James
*Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mian M. Mansha
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Oren
Sally A. Painter
Ana I. Palacio
*Kostas Paptazopoulos
Alan Pellegrini
David H. Petraeus
W. Devier Pierson
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
Gil Tenzer
*C. Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik

*Executive Committee Members

List as of January 5, 2022