JOHN C. GANNON, RICHARD A. MESERVE, AND MARIA T. ZUBER

Reconsidering Research Security

Research security isn't only about defending against external threats; it also requires ensuring that the United States remains a leader in global innovation by supporting the people and infrastructure that fuel it.

The United States' global leadership in research was built on the foundation of substantial government investments in science and technology (S&T) made during World War II. In the subsequent decades, S&T has been the critical means by which the United States has enhanced security, grown its economy, and nurtured improvements in its citizens' quality of life. The new markets, industries, companies, and military capabilities that emerged from greater S&T capacity have compounded to make the United States one of the most secure and economically prosperous nations on earth, generating more than 20% of global gross domestic product with only about 5% of the world's population.

However, America is no longer preeminent in all fields of fundamental science. Other countries have taken notice and are actively seeking to follow the path blazed by the United States. China in particular has a declared national goal of becoming the world leader in certain critical fields, including quantum computing, artificial intelligence and machine learning, biotechnology, microelectronics, and advanced manufacturing. These fields are likely to provide the foundation for future economic growth and national security, and China is making large investments in them—exceeding US investments in some cases.

With its growing S&T labor force, China may well have already obtained peer status or even drawn ahead of the United States in some fields. According to research from Georgetown University's Center for Security and Emerging Technology (CSET), China has made significant strides in research productivity, particularly in artificial intelligence, and is now the top producer of science, technology, engineering, and math (STEM) research globally, both in terms of total number of papers and number of highly cited papers. Though uneven in quality and impact, the output of published articles in science and engineering by Chinese researchers is nearly double that of the United States.

We spent the last four years as cochairs of the National Science, Technology, and Security Roundtable at the National Academies of Sciences, Engineering, and Medicine, sifting through progress reports; briefings and publications from federal research agencies in defense, energy, health, and science; and classified and unclassified briefings from law enforcement and intelligence communities. Speaking not for the roundtable, but as individuals, we became convinced that the Chinese government has pursued scientific progress through significant investment in China's national capacity *in addition to* targeted illegal or duplicitous actions to obtain knowledge on scientific and technical matters from researchers in the United States and elsewhere. In other words, although China's illegal appropriation of research ideas, results, and know-how has gotten a lot of attention in the United States, a broader view shows that the primary threat to US competitiveness lies in China's increasing scientific prowess. Thus, we believe the US response to counter China's advance must address not only the theft of intellectual property and other illicit activities, but also take measures to make the US scientific enterprise more competitive by investing in people and infrastructure.

This view contrasts with the agenda of the Department of Justice's China Initiative, which began in 2018 during the first Trump administration and remained active through 2022. The China Initiative focused largely and controversially on theft and espionage. In a speech after the Department of Justice (DOJ) ended the initiative in 2022, Assistant Attorney General Matthew Olsen acknowledged that civil rights groups felt that the initiative "fueled a narrative of intolerance and bias," suggesting that people from China or of Chinese descent were treated differently. He pledged "to take an active supervisory role in the investigations and prosecutions" and to "work with the FBI and other investigative agencies to assess the evidence of intent and materiality" to determine "whether criminal prosecution is warranted or whether civil or administrative remedies are more appropriate." This change in approach helped to stabilize the science-security relationship by engaging DOJ directly and more frequently in the disposition of problematic cases. However, further structured guidance was required from the White House on implementation of National Security Presidential Memorandum 33 (NSPM-33), which aimed to harden defenses against foreign interference, clarify disclosure requirements, and incentivize collaboration between the FBI and academia on research security.

Consensus on a dynamic threat

As awareness of China's threat grew within national security and law enforcement communities, academia initially gave the impression that it was caught off guard on the growing concerns about China and other cyber adversaries. In early meetings with the FBI, senior agents expressed frustration that US researchers did not appear to grasp the risks of welcoming foreign researchers to their campus labs. Researchers, in turn, emphatically defended the academic community's reliance on foreign STEM talent. As roundtable meetings proceeded, scholars and university administrators frequently asked for proof of claims by law enforcement that some academics were unconventional collectors acting on behalf of the Chinese government to pirate research results or expertise.

As these conversations took place over the years, we observed that they were most productive when universities already had a relationship with law enforcement—for example, when there was previous collaboration on security for sports events. Unsurprisingly, conversations were most fraught when the university's first interaction with the FBI was related to China Initiative investigations. Interestingly, we felt that academics had more common ground in briefings with the CIA than the FBI. Although agency members expressed deep concern about foreign interests, CIA agents, like academics, are fundamentally analysts, in contrast with FBI agents whose modus operandi is to investigate crime. Toward the end of our four-year mandate on the roundtable, however, the communities got to know each other and the cultural barriers between the law enforcement and research communities began to dissipate.

Another thing that struck us was that even though law enforcement focused on government-funded academic research, startups play an underrecognized and vulnerable role in translating basic research. Startups are often pivotal stops along the pathway from fundamental research in academic labs to the commercial applications of technology that can be developed for national security. This is a contrast to the postwar model of so-called linear research, with clear distinctions between commercial and security applications. Furthermore, today's fundamental research often creates a foundation on which a spectrum of diverse applications can be based. For example, advances in biotechnology, such as gene editing tools, can enable advances across domains including medicine, agriculture, and energy—and may move from commercial realms to security. So Chinese collection activity in a startup may include not only the details of a specific technology application, but also the fundamental research underlying it, which may have been done on university premises. However, neither law enforcement nor academic research decisionmakers have fully grasped the implications of these new and protean dynamics.

Investigative efforts by federal research agencies have revealed hundreds of cases involving grant fraud, theft of ideas and know-how, and foreign funding of research already supported by a federal agency. However, research by the bipartisan nonprofit Center for Strategic and International Studies ultimately uncovered few cases of espionage in academia. Instead, espionage cases investigated under the China Initiative were overwhelmingly associated with key government agencies, industry, or national labs. Our meetings with members from the private sector revealed that industry is taking ever more stringent actions to protect IP and trade secrets from disruption and theft by foreign entities, including defending against cyberattacks, which are of great and growing concern.

Given the vulnerability of industry, why has the conversation focused so intensively on academia? One reason is that academia plays a critical role in the promotion and defense of open science—yet, ironically, has limited access to current and reliable government information on threats to national security. This contributed to DOJ and law enforcement coming to see academia's open research model as susceptible to—and unprotected from—foreign interference. Academia, for its part, turned up the dial on defending open science, robust international engagement, and vigorous pursuit of foreign talent as vital to US research competitiveness.

But during the period of our study, we also saw the academic community recognize the need to put safeguards in place to counter foreign threats. We saw the DOJ/FBI respond, first in principle and incrementally in practice, to the existential importance of open science to US national security. In his speech after the China Initiative was suspended in 2022, Assistant Attorney General Olsen said, "Safeguarding the integrity and transparency of research institutions is a matter of national security. But so is ensuring that we continue to attract the best and the brightest researchers and scholars to our country from all around the world—and that we all continue to honor our tradition of academic openness and collaboration."

Agreement in principle, of course, does not remove conflicts in practice. One area of disagreement, for example, relates to the threat of illicit foreign appropriation of fundamental research and whether this threat warrants a blanket restriction of collaborations with foreigners. Decisionmakers from the scientific enterprise foresee that such a strategy, if applied broadly, would entail significant risk to US scientific capabilities. International collaborations are increasingly the norm, and excluding American researchers would compromise the advancement of the US scientific enterprise. Moreover, foreign-born researchers are a crucial element of US scientific competitiveness. In 2021, foreign-born workers (regardless of citizenship status) accounted for 19% of the STEM workforce. And nearly 60% of doctorate-level computer and mathematical scientists—fields associated with critical and emerging technologies—were born outside the country. Trying to protect against intellectual property theft by taking a simplistic approach to collaboration with foreign-born researchers could undermine US competitiveness in the future.

Response to the threat: defensive measures

Over the past six years, academic and federal research entities have taken significant steps toward greater security. For example, NSPM-33, issued by the Trump administration and revised and implemented by the Biden administration, set government agency–wide guidelines to safeguard federally funded research from foreign influence where appropriate, ensuring that sensitive work in American labs remains secure. And many universities, on their own and in response to explicit federal guidance, have implemented research security programs. The FBI is collaborating on the development of research security programs at multiple universities and has begun to reach out to the Asian American academic community to address concerns about discrimination. And the National Science Foundation is piloting a new decision process to assess research security issues in connection with the review of grant applications.

In general, the community is shifting toward best practices, including closer collaboration between academia and law enforcement. Building on this risk-based approach, the science and security communities should create mechanisms for collaborating on the setting and execution of policy. When the national security community concludes that elevated controls should be considered, working scientists and university administrators should be involved to identify effective solutions and, at the same time, to push back against measures likely to damage the US research enterprise. The scientists may even identify areas that are worthy of concern for economic or national security reasons, but of which the security community is unaware.

A similar collaborative approach to analyzing risks should be applied to the designation of Controlled Unclassified Information (CUI), or information produced or owned by the government that doesn't meet the criteria for classification but still requires protective measures. The controversial CUI marking is confusing to many people and, more seriously, disruptive to open science. The CUI designation should be revisited by the government with the objective of limiting its scope, achieving consistency in application, and providing clear guidance as to how to handle such information. In cases where restrictions are imposed, open research should be allowed to proceed if the researcher and the funding agency reach an agreement on measures to mitigate risk, such as restricting dissemination of information relating to limited aspects of the work.

Importantly, a strengthened risk management process should also include much deeper engagement with the private sector. The current focus on universities reflects, in part, the federal government's capacity as a major funder to exercise some control over academic research. In recent years, however, the private sector has played a larger role in fundamental research, both as a source of funds and as a research performer, resulting in less government involvement in such work. In some fields (e.g., artificial intelligence and biotechnology), research by the private sector bears a strong connection to national and economic security, which means there should be much deeper engagement with the private sector regarding threat mitigation, information sharing, and protection of research from foreign interference.

Along these lines, startups should be brought into the risk management policy process. Universities may be a party to licenses that derive from research on their campuses, but they do not have transparency into—or authority regarding—investors in startups. A foreign entity could gain access to sensitive research by investing in a startup even before the company obtained a license for the technology from a university. Because the startup would not have rights to the technology at the time of the investment, there would be no necessary review by the federal Committee on Foreign Investment in the United States. This "hole" in the protection of research of economic or national security importance should be examined. Moreover, perhaps greater scrutiny of investments in startups with rights to sensitive technology should be undertaken.

In sum, the United States must continue to implement enhanced protections against a dynamic and evolving foreign threat by building an agile, collaborative response. This would contain the threat, but not remove it: China has advanced cyber and AI capabilities and an unmatched capacity to interfere.

Building an offense: investing in people and tools

Defense is necessary, but it is not enough: Strengthening the foundation of the S&T enterprise from within will require investing in the future workforce and providing the foundation for scientific and technological advances in the future. Decisionmakers in government and academia must create stronger incentives for young people to pursue STEM careers and ensure that all students, from all communities and regions in the country, have the support they need to thrive in these fields. And the nation must invest in education and training at every level, starting with kindergarten and continuing all the way up to postdoctoral researchers.

Investment in education needs particular attention because research funding dynamics are shifting in ways that disadvantage education. Between 2011 and 2021, 87% of research growth came from the private sector, where little funding goes toward training the future workforce. And recent increases in federal investments associated with the CHIPS and Science Act, the Inflation Reduction Act, and the launch of the Advanced Research Projects Agency for Health provide much needed, once-in-a-generation boosts to research involving semiconductors, clean energy, and innovation in physical sciences and health. But caps on the discretionary part of the federal budget in fiscal year 2024 have put these gains at risk—and specific carve-outs for universities are scarce.

Even when students graduate with STEM degrees, recent research has shown that only a third of them get employment in STEM jobs. This statistic raises several questions. Is the problem an oversupply of graduates compared to positions in their field? Is the issue how STEM occupations and graduates are defined and categorized? Or are STEM graduates simply attracted by other professions? In any case, the US research enterprise relies heavily on the labor of graduate students and postdoctoral researchers, and it requires new strategies aimed at retaining these workers. Too many young scientists struggle to make ends meet because graduate and postdoctoral stipends at some universities, particularly in areas with high costs of living, are below a living wage. To attract and retain top talent, the research enterprise must ensure that graduate students and postdoc researchers are better paid and on pathways to rewarding careers in academia as well as industry. Without support, university STEM expertise could dwindle, potentially affecting research as well as the overall S&T workforce in the longer term.

As the United States works to increase the pool of domestic STEM talent, it should recognize that recruiting foreign STEM talent and welcoming their continued involvement in the S&T enterprise is also in the national interest. Government and the research enterprise must grapple thoughtfully with the US research system's reliance upon foreign-born scientists. When the China Initiative was active, investigations and security measures aimed at foreign-born scientists and Asian Americans led to fear, mistrust, and a growing sense of alienation within the scientific community. There should be a forceful response to continuing reports of discrimination and alleged border harassment of traveling foreign students and faculty. And barriers to attracting foreign researchers to the United States should be eased by eliminating visa impediments and other immigration obstacles to maintain the competitiveness of the system as a whole.

Finally, cutting-edge research requires cutting-edge tools—such as advanced instrumentation, modern wet labs, and access to high-performance computing capability—which enable the expansion of the boundaries of knowledge. This includes shared facilities for academia-industry collaboration and access to state-of-the-art equipment. And restructuring governmental research contracting and business practices to reduce bureaucratic burdens on researchers can work synergistically with modernized infrastructure to achieve greater efficiency and effectiveness.

It's time to channel resources into cultivating talent, supporting researchers at every stage of their careers, and providing them with the tools they need to succeed. By doing so, America strengthens its ability to compete in a world in which peer competitors are closing the gap.

An investment in the future

Research security isn't only about defending against external threats; it's also about ensuring that the United States remains the leader in global innovation by supporting the people and infrastructure that fuel it. As we have argued, by addressing concerns about security while making stronger investments in people, the nation will be positioned to match and even exceed its remarkable scientific achievements of the past few decades.

Still, the role of S&T as a critical national security asset urgently requires new thinking. The United States will face unprecedented challenges: intensifying foreign competition, the steadily growing role of the private sector in scientific research, and domestic disputes about how to govern a vast, decentralized, and complicated research enterprise. Foreign competition and interference, especially from China, will sharpen. At home, major industries fueled by leading technologies will likely have growing government influence and will increase their resistance to regulation as an obstacle to innovation. However this plays out, the S&T enterprise will need to develop and convey a more forceful, vocal, and united front in defense of open science and international engagement.

John C. Gannon *was, prior to retirement, chairman of the National Intelligence Council, the CIA's deputy director for intelligence, president of the Intelligence & Security sector at BAE Systems, and adjunct professor of security studies at Georgetown University.* ***Richard A. Meserve*** *is senior of counsel at Covington & Burling LLP and president emeritus of the Carnegie Institution for Science. He was previously the chairman of the International Nuclear Safety Group and chairman of the US Nuclear Regulatory Commission.* ***Maria T. Zuber*** *is presidential advisor for science and technology policy and the E. A. Griswold Professor of Geophysics at the Massachusetts Institute of Technology. She cochaired President Biden's Council of Advisors on Science and Technology and chaired the National Science Board during President Trump's first term.*