PETER SCHIFFER AND FREDERICK R. CHANG

How Openness Could Strengthen Academia's Partnerships with the Intelligence Community

Starting with Vannevar Bush's seminal 1945 report, *Science, the Endless Frontier*, the federal government has invested significantly in support of fundamental research at universities across all areas of science and engineering. For even longer, government agencies have partnered with universities to perform research in support of agency missions and to meet national needs. For example, the National Institutes of Health support health-related research, the Department of Agriculture supports agricultural research programs, and the Department of Energy supports energy solutions. And of course, since World War II, the Department of Defense has invested in defense-oriented research at universities.

Strong government-university research partnerships can be especially impactful to one sector of the government that is somewhat invisible to outsiders: the US intelligence community (IC). The IC comprises 18 organizations and agencies within the executive branch of the federal government—all with the shared mission of supporting the government's understanding of the world by collecting, analyzing, and disseminating intelligence. Fulfilling this mission requires access to the most advanced science and technology (S&T) available. Today, the S&T landscape is evolving quickly, and it offers new opportunities and incentives for the IC to develop partnerships with academia. Done properly, enhancing such partnerships will benefit both national security and the academic research enterprise. Somewhat counterintuitively, we also argue that the open nature of academia presents special opportunities for higher impact.

Recent shifts in the global technological landscape have several facets that are relevant to the IC. One well-studied trend has been toward effective investments by other countries in their own science and technology-based innovation ecosystems. Additionally, commercial entities in the United States and abroad are now among the world leaders in multiple fields of importance to the intelligence community, including microelectronics, artificial intelligence, quantum computing, synthetic biology, and genomics. And finally, new possibilities for gathering intelligence are becoming available through freely available digitized information—known as open intelligence—which can be mined for deeper meanings and contexts.

At the request of the Office of the Director of National Intelligence (ODNI), the National Academies of Sciences, Engineering, and Medicine (NASEM) conducted a consensus study released last year that explored "ways in which the IC might leverage the future research and development ecosystem." The study, in which we both participated, concluded that, to maintain its capabilities and serve the nation, the IC must continue to innovate—potentially reorganizing its S&T leadership while forging new partnerships with industry, other sectors of the government, and international entities. Critically, the study also recognized the need for the IC to build stronger connections to academia in order to develop the cutting-edge research, the technically savvy future intelligence workforce, and the kinds of creative insights that the IC requires to fulfill its missions in a rapidly changing world.

There are significant barriers to broader engagement between the IC and academia. Historically, the culture around intelligence is one of secrecy, which runs counter to the open culture of the research university. The low public profile of the IC agencies also does not encourage spontaneous inquiries from university researchers seeking funding, input, or collaboration. Furthermore, much of the S&T work performed by the IC is classified, which excludes the large portion of the academic workforce without the necessary security clearances. In particular, university researchers who are foreign nationals are almost always ineligible to obtain clearances and often cannot even work with export-controlled technologies, such as certain types of sensors or software.

Following the NASEM study, we were both interested in further exploring IC-university research partnerships, how they could be expanded, what obstacles must be overcome, and what special characteristics of the two ecosystems can best be leveraged together.

How the intelligence community can better engage academia

A straightforward route toward greater engagement will be for the IC to expand outreach opportunities for those academics who are more immediately ready to partner. One recommendation from the NASEM report was to increase the number of temporary assignments, commonly known as rotational positions, for academics to work within the IC S&T ecosystem. Such rotations might be most appealing to academics if they required either no security clearance or only a lower-level clearance that comes with fewer restrictions. To foster more contacts, the IC could enhance its efforts in both organizing and attending conferences and other communication venues for networking and meetings between its own experts and academics. The IC could also sponsor more student programs, such as those that have been operated by the ODNI through the Intelligence Community Centers of Academic Excellence and the National Security Agency (NSA) through its National Centers of Academic Excellence in Cybersecurity, which engage with university faculty and students to help fill significant workforce needs. Similar partnerships have also been developed by the Central Intelligence Agency through its Signature School Program.

Separately, the intelligence community could increase direct funding to the academic community to perform high-impact foundational research in strategically important areas. One possibility would be to expand programs already in place through the Intelligence Advanced Research Projects Activity (IARPA), which directs efforts toward the specific needs of IC agencies. IARPA supports a broad range of research projects including detection of biothreats, data analytics, and many similar topics in which academic researchers have deep expertise. Another possibility would be to build on the NSA's Science of Security and Privacy Initiative, which funds small, multidisciplinary "Lablets" at partner universities. These efforts focus on foundational cybersecurity science that will underpin future cybersecurity efforts. Such programs could be expanded, considering that there are important S&T topics that are of interest to many agencies of the IC. Collaboration between multiple agencies with academic institutions could potentially form the basis for cross-agency collaborations of the sort envisioned in the NASEM committee report.

The science and technology landscape is evolving quickly, and it offers new opportunities and incentives for the intelligence community to develop partnerships with academia.

An increasingly important opportunity for all of these avenues of engagement can be found in the truly enormous quantities of open information that are freely available on the web. Universities have been leaders in leveraging open data in pursuit of deeper understanding, supporting the broad goals of a recent White House memo. With the costs of both data storage and computing cycles dropping continuously, accompanied by the advent of ever more powerful artificial intelligence tools, such open source intelligence gathering has the potential to revolutionize many of the IC's activities. Thought leaders such as the Center for Security and Intelligence Studies have noted that integration of such open source information into the IC's analytic tools is a challenge because it represents a considerable paradigm shift. This is a space where

The intelligence community could increase direct funding to the academic community to perform high-impact foundational research in strategically important areas.

academic researchers could help the IC without the barriers posed by security clearances while also building analytical tools that can be applied to other issues, such as environmental and social challenges.

All of these activities would both provide the IC with access to the latest research and insights from academia while also giving university scholars more opportunities to apply their expertise to an unusual set of practical problems. Although some academics will have no interest in such engagement, others will welcome the new intellectual challenges and venues to expand their research impact and contribute to the national interest. Work on mission-driven IC-related problems offers academics opportunities to expand their research perspectives and explore new approaches in more basic research programs. We note that the Department of Defense uses similar methods to maintain robust working relationships with universities, providing extensive evidence that all of these approaches can work well for topics that relate to national security.

How academia can engage the intelligence community

Although the IC has some clear paths toward enhancing interactions with university research, relatively little attention has been paid to how the academic research ecosystem might reciprocate the efforts. One route for potential university partners would be to add to their existing capabilities to perform classified research and to develop programs designed toward the current needs of the IC. Many universities have the capacity to perform such research now, either in stand-alone facilities or through formal structures such as the Department of Defense University Affiliated Research Centers, some of which host work for the IC already. These centers often involve students in defense-related applied research, introducing them to career options in national security and building a potential workforce.

From our perspective, however, a more far-sighted approach would be for universities to build on their strengths as forums for intellectual exchange, maintaining and supporting the open character of university research in work related to IC missions. Universities can leverage their traditional strengths of academic freedom and openness that have brought them to their current global preeminence, and they can promote that strength in partnership with the IC. Universities should continue to advocate for an open research ecosystem in which they work collaboratively with the IC, with research kept unclassified to the maximum extent possible—as has been the national policy since the 1985 National Security Decision Directive 189. This open culture allows university researchers to reach across disciplinary boundaries and explore new partnerships and avenues of research, and it dovetails with the increasing importance of analyzing and understanding open data.

Most importantly, the US university system should maintain its long-standing reputation as a beacon for top-notch S&T talent from around the world. For generations, many of the best students from across the globe have come to the United States and thrived in the university system's welcoming environment. Recent concerns about national security have, however, led to some federal actions that have the potential to discourage global engagement and endanger the strength of the US research ecosystem as a world leader. In particular, in an increasingly polarized world, the expectations of collaborative work with scientists across national boundaries are changing. There are real security concerns, and they must be taken seriously as other nations target the US research ecosystem in ways that are not consistent with the country's national interests. On the other hand, the wrong balance of responses to those concerns will deny the United States access to the best minds in the world and will suppress critical international collaborations. Only by maintaining the globally open and welcoming university research environment that has been fostered since the time of Vannevar Bush will universities continue to offer the intellectual resources that the IC needs.

Peter Schiffer *is the Frederick W. Beinecke Professor of Applied Physics and professor of physics at Yale University.* ***Frederick R. Chang*** *is the Inaugural Bobby B. Lyle Centennial Distinguished Chair in Cyber Security at Southern Methodist University.*