Dr. Maria T. Zuber

Vice President for Research, Massachusetts Institute of Technology

Written Testimony

House Permanent Select Committee on Intelligence

Subcommittee on Strategic Technology and Advanced Research

February 12, 2020

Mr. Chairman, Ranking Member Stewart and Members of the Committee,

Thank you for inviting me to testify on this critical subject – how to ensure the intelligence community has the technology it needs to protect our country. This Subcommittee clearly appreciates how important technological supremacy has been, and is to U.S. security, so I will not spend time making that case.

One way to frame the subject of this hearing is, "How can the U.S. maintain and build on its current strengths to help the intelligence community (IC)?" I believe those strengths include world-class universities, an open research system, and the ability to attract and retain top talent from around the world. The federal government can do more to strengthen those assets and ensure that the IC is benefiting from them.

My recommendations fall into three categories – enhancing U.S. research in key technology areas; improving interaction between the IC and our research system; and ensuring the U.S. remains a magnet for top talent.

RESEARCH

Keeping the U.S. ahead in critical technologies like artificial intelligence and quantum computing requires strategy and funding. Estimates of Chinese investment in AI, for example, vary widely, but even the most conservative estimates find China at least at spending parity with the U.S. and committed to becoming a world leader in the field.

The federal government needs a visible, focused and sustained effort in key research areas. That would entail a significant increase in funding for fundamental research at universities, targeted at problems like developing new algorithms that would enable machines to "learn" with less data. That increase should not come at the expense of the rest of the research system.

It is encouraging to see the Trump Administration and Congressional proposals that recognize the need for more funding. But these budget and authorization proposals need to be followed up with actual appropriations. The scale of the commitment needed to make a difference is going to be hard to achieve without in some way placing this investment outside the constraints of the normal budget process. That's what it means to be a priority.

Ideally, increased funding would be paired with bureaucratic reforms to improve focus across agencies. One way to turbocharge existing efforts would be to create a new directorate at the National Science Foundation with Defense Advanced Research Projects Agency (DARPA)-like authorities that would focus on critical technologies. The directorate could provide funding to other agencies, as well as to universities and consortia involving industry. When witnesses were asked about this idea at a January 29 hearing of the House Science Committee, all responded positively. The witnesses were former Google CEO Eric Schmidt, National Science Board Chair Diane Souvaine and Chaouki Abdallah, the executive vice president for research at the Georgia Institute of Technology.

Regardless of whether a new entity is created, the IC's own research agencies need to be adequately funded. The research arms of the intelligence agencies have not increased substantively even as defense R&D has boomed. Why not?

INTERACTION

The technologies needed to defend the U.S. increasingly originate in the civilian sector. Numerous studies have underscored this point, including, "Innovation and National Security: Keeping Our Edge," a report from a task force of the Council on Foreign Relations, on which MIT President Rafael Reif served (https://www.cfr.org/report/keeping-our-edge/).

Therefore, the IC needs to be better positioned to help shape research questions in academia and industry and to capitalize on research results. That requires more talking together and working together.

For example, the Intelligence Advanced Research Projects Agency (IARPA) could enhance interaction by working more with agencies like the National Science Foundation and the National Institutes of Health (and vice versa) to think about how open research could advance the IC's goals.

Also, the IC on its own, or in collaboration with other agencies, could run more challenges in key areas. IARPA already makes frequent use of prize challenges to cost-effectively draw innovations from the private sector (as does DARPA); other IC research organizations could also be making use of the prize authorities provided by the *America COMPETES Act*. The IC could establish regular technical challenges that articulate and address IC needs in areas such as image analysis; deception detection and counter-deception; and open-source data discovery, as well as in emerging technologies such as brain-computer interface and quantum encryption.

Whether working on its own or in collaboration with other agencies, the IC needs to streamline its procedures for working with universities. The IC contracting process is slow, typically taking more than six months for contract awards. The IC needs to empower its officials to award contracts quickly with more risk tolerance. Most of the contracting process aims at reducing protest risk, but that risk is quite small with R&D contracts. Essentially, today the IC treats a $1 million research contract with the same level of oversight as it treats a $1 billion acquisition. That should change.

As noted above, working together needs to be encouraged. The IC could do much more to rotate its members through universities and federal labs by granting sabbaticals or using other mechanisms, such as joint research projects.

There is simply no substitute for having people work side-by-side. This can be done, indeed must be done, without changing the open culture of universities. Last year, MIT signed a five-year agreement with the Air Force to operate what we're calling an AI Accelerator. Under this program, Air Force staff are working both on campus (where research is open) and at Lincoln Laboratory (which MIT runs and which is secure) on problems of interest to the Air Force and MIT. Thus far, the Air Force and MIT are collectively delighted with the quality of proposals received and with the productive spirit of collaboration. The AI Accelerator is a model the IC should consider.

Such cooperation could be especially appropriate to help sort through the ethical questions posed by AI and other new technologies. Those research questions require attention not only from experts in the social sciences and humanities, but also from technical experts, who are working, for example, on minimizing bias in AI algorithms. MIT is putting increased emphasis on such work, which will be a focus of our new Schwarzman College of Computing.

Let me emphasize again the need for the bulk of this work to be open. Greater cooperation should not be an excuse to find new ways to limit research exchanges. We strongly endorse the findings of the recent report "Fundamental Research Security" that the JASONs performed for the National Science Foundation

(https://nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf).

The report reaffirmed the longstanding policy enshrined in National Security Decision Directive-189 that fundamental research should generally be unrestricted, and that when restrictions are needed, classification should be the mechanism. The government should not be creating an array of new "gray areas" that are confidential but unclassified.

Just as IC members should be enabled to spend more time in academia, academics could be encouraged to spend time in the IC. The IC should make better use of the Intergovernmental Personnel Act (IPA) to draw in experts from academia to serve in key term-limited science and technology roles within government.

One current barrier is unfamiliarity – many IC human resources offices are unfamiliar with the IPA. Another barrier is the blanket requirement for top secret (TS/SCI) security clearances. Currently, by default, employees of most IC S&T organizations need to be fully cleared to TS/SCI before they can begin work. That typically requires waiting a year before starting work, which is impractical for most people, and severely strains staff planning. One possible approach to fix that would be for the IC could bring in personnel who pass preliminary background investigations and have them work on unclassified projects – which is the bulk of IC R&D work – while waiting for their clearances.

More can also be done to increase research interactions between the IC and private companies, something that is of particular interest to our researchers at Lincoln Laboratory. Current barriers include IC adherence to specific cost-accounting standards, timelines associated with the bid and award process, intellectual property restrictions and required software certifications. These are especially difficult hurdles for smaller companies with limited experience working with the IC.

The IC should experiment with Other Transactions Authority and other mechanisms that agencies like the Department of Defense and NASA employ to make it easier for companies to collaborate.

Other models to investigate are the Air Force's use of its Small Business Innovative Research (SBIR) funding to support same-day small contract awards and its establishment of AFWerx to facilitate greater engagement with the private sector to meet Air Force technology needs.

A more novel approach might be to establish, in regions where high concentrations of IC-technology-relevant companies exist, centers that offer "security as a service" support. These centers might include classified network access, meeting and collaboration spaces, and staff for processing security clearances.

TALENT

The U.S. will not succeed if we alienate or turn away ambitious, brilliant students and researchers. Obviously, those who are coming to our country need to be vetted appropriately by the federal government, but that process has to be targeted and rational; it cannot look like mere harassment.

The latest statistics from the National Science Board show that foreign students account for more than half the U.S. doctoral degrees in engineering, mathematics and computer science, with more than half of those foreign students coming from China, India and South Korea. This is not a new situation. What is new is that fewer of them are staying – although most still remain. NSF found that 84 percent of the doctoral students from China were still in the U.S. five years after receiving their degree. We need to get more U.S.-born students into these fields, but even when we succeed at that, attracting and retaining top students from overseas will still be an asset.

As the federal government and universities rightly shore up our systems to prevent improper and illicit losses of technology, we need to be sure our actions address the actual problems. Foreign students have not featured prominently in cases of technological theft. Yet they are frequently the target of restrictive proposals. New policies should be focused on real security gaps, not on classes of people who help the U.S., but are easy to demonize or restrict.

I am attaching comments MIT recently provided to the White House Office of Science and Technology Policy that describe in greater detail the approach we think the federal government should be taking to enhance research security at universities without counter-productive consequences.

One principle we mention with regard to foreign students is that once allowed into the U.S., foreign students should be treated like all other students. They should not be subject to additional restrictions except where controlled technology is involved. Restrictions both make it harder to attract students and reduce their value if they still enroll.

The intelligence Division of the *National Defense Authorization Act of 2019* includes a provision that could either help or harm the ability of universities to contribute to our national security, depending on implementation.

If the lists required of the Office of the Director of National Intelligence by Section 5713 provide more specific information on threats and incidents than is currently available, that would be helpful. But if the provision results in a proliferation of general lists of research areas with security implications or of foreign institutions that theoretically pose a problem, then the law could simply make research progress more difficult without enhancing security.

Our general view is that the U.S. faces new challenges and competitors, but we are well placed to succeed if we get the most from our unrivaled strengths. The heart of our strategy must be confidence in ourselves, not fear of others.