Terry Benzel
Associate Editor in Chief

Research and Industry Partnerships in Cybersecurity and Privacy Research: New Frontiers or Fueling the Tech Sector?

Increasingly, tech industry giants are engaging in partnerships with academic researchers. This comes in three primary forms:

- industry partnering with government funding organizations, such as the National Science Foundation (NSF)
- academic researchers, faculty, and graduate students who are working in industry part-time or on a leave of absence from academia
- academic institutions entering into cooperative R&D agreements with industry partners and/or other academic institutions.

There are other forms of partnerships, such as those among multiple government agencies, international partnerships, nonprofit foundations, and consortiums, such as the Hewlett and Simmons Foundations. Each of these has a different flavor from the three cases listed and are not covered here.

Partnerships and Cybersecurity: Can Researchers Go It Alone?

Cybersecurity is now a constant challenge for every facet of civilized society. We have become completely dependent on cyber capabilities and, as a result, highly vulnerable to wide-ranging threats. Despite years of research, however, we are still at the losing end of an asymmetric battle. As a nation, we must support new forms of R&D and ensure that the resulting advances are grounded in the real-world threats facing us.

I am a firm believer in a balance between far-reaching academic work of a theoretical nature and the R&D motivated by applications known as *use-inspired research*. I have always felt that understanding the hard problems facing industry today makes us better researchers.

On the other hand, if we allow ourselves to concentrate too closely on academic research objectives (graduating students, publishing, or obtaining tenure), then our research runs the risk of being too narrowly focused (minimum publishable unit syndrome). This is particularly risky for cybersecurity research, which starts to address niche topics, with the result of increasing rather than decreasing security risks.

Our adversaries are also engaged in R&D, planning their attack scenarios. They are looking across multiple threat vectors for system vulnerabilities, within and across different technologies, and picking targets for their strategic value—not simply because they are academically popular or technically easy marks. In other (adversarial) countries, the governments largely dictate the R&D that their academics pursue. The U.S. government has a much different relationship with its academic and industry partners.

While top academic institutions in the United States hew to time-honored traditions of excellence, they also rely on extramural funding for their research programs. The sponsors of those programs do influence the topics that academic researchers—faculty

Digital Object Identifier 10.1109/MSEC.2021.3094313
Date of current version: 3 September 2021

 1540-7993/21©2021IEEE

and students—pursue. At tier-one research universities, there is a high expectation that the research conducted by faculty and graduate students will be funded and relevant to solving problems of great importance to society, with the results transitioned via licensable patents or direct technology transfer [e.g., co-ownership of intellectual property (IP) with government and industry partners]. This culture provides the impetus to perform research relevant to society, but it might also narrow the horizon or topics to be addressed.

Overall, the research community environment helps create a balance of research that helps ensure substantial progress away from a narrow cybersecurity research focus. Federal agency sponsors have been steering researchers toward cybersecurity issues that are critical to national, homeland, and economic security.

One result is more breadth, collaboration, and partnering in cybersecurity research. Another, perhaps more critical, outcome is a shift away from existing commercial cybersecurity problems to those that are not yet subject to rigorous work. The NSF is pursuing this strategic approach through its frontier-, large-, medium-, and center-focused Secure and Trustworthy Cyberspace program and a new focus on partnerships.

Still, studying broadly within our own disciplines is not enough. Cybersecurity is not solely an engineering discipline. It requires deep involvement from economists, sociologists, anthropologists, and other scientists to create the holistic research agendas that can anticipate and guide effective cyberdefense strategies. This reality creates an environment that is rich for collaborations, partnerships, and new forms of commercial and academic working relationships.

Two recent reports from the NSF Directorate for Computer and Information Science and Engineering (CISE) Advisory Committee (AC) examined issues related to new forms of research and relationships with industry for computer science research broadly. The NSF CISE Vision 2030[1] looks out a decade and beyond to understand the key opportunities and challenges facing the NSF CISE. The report explores three key questions:

- Where is the computing field going over the next 10–15 years?
- What are the potential opportunities, disruptive trends, and blind spots?
- Are there new questions and directions that deserve greater attention by the research community and new investments in computing research?

In this context, the report raises issues of accelerating trends, human capital, and the changing environment of scientific research as challenges to address as the research community moves forward through the next 10 years.

"NSF CISE AC Report on Private-Sector Partnerships"[2] describes the NSF CISE experience with partnerships in multiple sectors, public and private. These partnerships have had multiple benefits for the CISE academic research

Digital Object Identifier 10.1109/MSEC.2020.3044407

community, including connecting researchers and students with current problems, industry expertise, and resources; accelerating research and its transition to practice; and spurring new innovations and fields of research.

The CISE AC formed a subcommittee to review the partnership landscape specifically from the research community perspective. The subcommittee and report focused on the CISE's current experience and direction in public–private partnerships and made recommendations to address challenges, operationalize the partnership process, address funding and IP models, and advance Broadening Participation in Computing as a key element of partnerships.

Both reports addressed cybersecurity specifically in places while covering the topics more broadly. The different approaches to academic–industry partnerships and working relationships described in these reports apply directly to cybersecurity and privacy as part of this larger context.

Context

To appreciate the contributions of these reports, it is necessary to establish the evolving context of computer science/cybersecurity research. Examining our universities and the major tech companies, it is clear that the private sector is engaging with academia at an unprecedented rate. As noted in a recent Computing Research Association report,[3] engagement between computer science researchers and industry has significantly increased. This is particularly true in the areas of cybersecurity, next-generation networking, and, of course, artificial intelligence.

Industry is starved for talent and needs to draw heavily on academia to keep up with the rapidly changing technology landscape. Not only do companies need skills and people power, but they also require insight into emerging disciplines, such as ethics, privacy and security, and the combination of social behavioral and computer science.

At the same time, industry investment in its own R&D is at a low point, having divested many corporate research labs in favor of more products and newly created services in an increasingly competitive market. Now, facing demands, industry has reached into the academic research community by luring scholars and graduate students to jobs or directly funding academic research for use in its offerings. Some researchers and companies have attempted to develop cooperative arrangements where faculty work one or two days a week for industry while remaining committed to the traditional activities of academia (research, publishing, teaching, and graduate student mentoring).

All of this increased engagement and these ad hoc agreements can be both a positive and negative. On the plus side, the research community gains access to massive amounts of data, infrastructure, and business insights. Conversely, the industrial focus may well prevent the research community from obtaining fundamental research breakthroughs and may reduce research talent production in the next generation through industry hiring. This situation is probably more widespread than we fully understand, and the long-term effect is not yet understood.

Research Community Partnerships With Industry

Historically, researchers were very clearly associated with either academia or an industrial or government research lab. In the last five years, this picture has shifted significantly. We now see researchers leaving academia for industry or engaging in dual (dueling?) appointments between academia and industry.

An obvious reason for this shift is the gap between academic and industry salaries. However, there are also important research-driven reasons behind the shift. Industry can offer researchers access to larger research groups, vital data, and rich research infrastructure. Sharing time between an academic appointment and a company can bring new opportunities for collaboration with industry researchers, graduate students, and teaching. However, such situations also run the risk of reduced engagement on the part of the academic, less availability for graduate students, and, most seriously, fewer fundamental open research results and publications.

Partnerships With the NSF

During this same period, the NSF, with leadership from the CISE, has developed strong public–private partnerships that have provided opportunities for the CISE to fund more research and encourage research focused on some of the hard problems facing industry today. All CISE partnerships with industry are based on a memorandum of understanding (MOU). In some cases, the companies send funds to the NSF; in others, the NSF makes an award to the university, and the company funds the project separately.

Initially, these partnerships were mostly bilateral, involving the NSF and a single company. More recently, the NSF CISE has developed extensive multilateral partnerships, with multiple industry partners contributing funding, data, infrastructure, and internal researcher collaborations to an NSF research program.

Since 2014, the CISE's investment of more than US$173 million has been matched by private-sector partners, with more than US$107 million and in-kind support. It is widely believed that the CISE partnerships have been beneficial to the research community. These include connecting NSF researchers with current applied problems, industry

expertise, data, and infrastructure as well as helping to accelerate research timelines and rapid technology transition.

The use of an MOU with partners is key. As described in the CISE AC Partnership report,[2]

> *these documents address (1) the area of joint research interest; (2) special review criteria (if any) to be used in the solicitation, review and selection processes; (3) a mechanism for the private entity to provide input into the NSF-led review process (ranging from observing the panel reviews to holding a separate review that provides input, e.g., those deemed most relevant to the entity's need); (4) nature and degree of involvement with awardees after awards are made, for example attendance at PI meetings, receiving reports; (5) amount of funding and how the private entity's funding will be awarded, e.g., via NSF, or separately to the awardee institution; (6) disposition of research products and intellectual property; (7) joint communication with the community; and (8) dispute resolution and termination; among other topics.*

Examples of NSF CISE bilateral partnerships include Intel Labs, VMware Inc., and Amazon. Currently, the NSF is engaged in several large multilateral partnerships, including the National Artificial Intelligence Research Institutes, which has multiple federal agencies, Accenture, Amazon, Google, and Intel, and the Resilient and Intelligent NextG Systems program, which includes multiple federal agencies and Apple, Ericsson, Google, IBM, Intel, Microsoft, Nokia, Qualcomm, and VMware.

These are prime examples of research topics that have enormous breadth inside and outside of academia with the potential for major societal impact. It is hard to imagine that any single company or federal research program could address the myriad research topics in each of these areas. It is a testament to the NSF CISE leadership that they were able to bring so many competing companies to the table to work together and with the research community.

The NSF has worked hard to address difficult issues of IP in the context of partnerships and stresses the importance of long-term precompetitive research as a motivator. Nonetheless, concerns around IP and longer-term closed researcher–industry collaboration should be monitored as the NSF explores these models.

However, in thinking about industry partnerships with the NSF CISE, it is important to keep in mind that the NSF funds more than 80% of all federal fundamental computer science research in this country. These funds are in increasing demand as computer science research permeates an increasing range of topics and disciplines.

The NSF CISE must strive to create and maintain the right balance between fundamental and industry-applied research. As tech giants take on an ever-increasing dominance in our society, the distance between all types of resources in our universities and those of industry is far greater than it has been at any time in the past.

Finally, we can all agree that accelerating research and enabling technology transfer is an important aspect of what we do. We need to invest in R&D that addresses real-world problems—including those we envision for the future. Not only does tech transfer advance commercial technology, but it also provides insights and hard problems to inspire new research. Partnerships, shared appointments, specific funded tech transfer activities, and opportunities for students are vital to the fundamental research of academia. I am glad to see the NSF CISE organization so vigorously engaged in creating partnership opportunities while also carefully considering the issues with codifying processes.

It is past time for a serious national conversation with the funding agencies, academic community, and industry. In light of national strategic cybersecurity concerns and the importance of privacy in our society, we must ensure the integrity of research in all guises while, at the same time, maintaining an openness of ideas, data, results, expertise, and people in the conduct of fundamental research.

So you tell me: Through research and industry partnerships, are we diluting fundamental research? Are we accelerating new ideas and research as well as facilitating tech transfer in national priority areas? Are we harming our key research institutions? ■

References

1. "NSF CISE Vision 2030: A vision for NSF CISE opportunities and challenges over the next decade," National Science Foundation, Alexandria, VA, Feb. 3, 2021. [Online]. Available: https://nsf.gov/cise/advisory/CISE_Vision_2030.pdf
2. "NSF CISE AC report on private-sector partnerships date TBD," National Science Foundation, Alexandria, VA. [Online]. Available: https://www.nsf.gov/cise/advisory.jsp
3. S. Patel et al., "Evolving academia/industry relations in computing research," Computing Research Association, Washington, D.C., June 2019. [Online]. Available: https://cra.org/ccc/wp-content/uploads/sites/2/2019/06/Evolving-AcademiaIndustry-Relations-in-Computing-Research.pdf