David M. Nicol

The Value of Useless Academic Research to the Cyberdefense of Critical Infrastructures

Like a barker in front of a carnival tent, the title was chosen to draw your attention! It is a play on the 1939 essay "The Usefulness of Useless Knowledge,"[1] written by Abraham Flexner, the first director of Princeton's Institute for Advanced Study. Flexner points out the foundational role that research for knowledge's sake plays in technology development. Although he stresses the need for research with absolutely no practical objective in mind, my argument is for the value of early-stage research that is relevant to an application domain but useless in the sense of not being close to transitioning to practical use. My emphasis is on research that helps increase the cyberdefense of critical infrastructures, such as electric power, oil and gas, transportation, and critical manufacturing. Although I don't expect arguments against the existence of this value, I believe that this kind of early-stage research is underappreciated by funders and industry, in part because these stakeholders don't yet see the role it can play in workforce development and outreach to industry. After fleshing out these points, I'll offer an idea that tries to address the problem.

Critical infrastructures of industrialized nations are vulnerable to attack on their digitized controls. Cyber-based threats are on the rise, with new threats circumventing existing protection. Furthermore, critical infrastructures are typically owned and operated by private companies, and defense of the critical infrastructures against cyberbased attack rests on these companies. Although the largest companies can allocate people and license software tools to maintain an active cyberdefense, much of the infrastructure is managed by small or medium-sized companies that cannot. This is problematic because infrastructures like the power grid and manufacturing systems are composed of independently owned subsystems that are coupled. A successful cyberattack against a weakly defended company can be leveraged by an attacker to impact the system as a whole.

Against these threats, what is the value of early-stage research? Both the U.S. Department of Energy (DOE) and the Department of Homeland Security (DHS) invest in research for which there is a clear transition path to practical use and eventual commercial self-sufficiency. However, the expectation of transition exposes the assumption that prior research has already brought the state of knowledge to a point from which refinement, application, and transition are possible. One obvious value of early-stage research is helping to create starting points for later-stage work that transitions.

Perhaps less obvious, another benefit of early-stage research is in the training of students who end up working with cybersecurity in some critical infrastructure and training of others who pursue research careers in the area. For these purposes, the specific cybersecurity research problem a student pursues doesn't matter much, so long as the research problem is relevant to and informed by the operation of a critical infrastructure. Hires are made based on a student's potential; the student's research is preparation to work at a certain level of sophistication. Although (of course) student training occurs with research poised for transition, support for early-stage research as well increases the pool of new workers and, I will argue, increases the number of faculty prepared to assist critical infrastructure industries in their cyberdefense.

So there are at least two ways in which early-stage research can help address the threats. How is that research typically funded? In the

Digital Object Identifier 10.1109/MSEC.2019.2951835
Date of current version: 23 January 2020

United States, the National Science Foundation (NSF) plays a key and solitary role. The Cyber-Physical Systems (CPS) program in the Division of Computer and Network Systems is a natural place to submit proposals. The NSF puts award information online, and a search of CPS awards since 2013 shows a total of 372 grants, of which 11 have titles related to cybersecurity of critical infrastructures. Those 11 projects received a total of US$6.6 million.

The other natural NSF program for submissions is Secure and Trustworthy Cyberspace (SaTC) in the same division. A search of SaTC awards since 2012 yields seven out of 862 awards with titles related to critical infrastructure or cyber-physical systems, receiving a total of US$2.4 million. Of course, both programs have a much wider scope than cybersecurity of critical infrastructure, and these figures say nothing about the topics of proposals not selected for funding. Still, at my university, US$9 million would fund fewer than 35 students during those seven years, if each were supported throughout a four-year Ph.D. program. A nationwide yield of five Ph.D. students per year is a tiny investment in early-stage research against the backdrop of a critical need.

How could the size of this investment be boosted, and whose responsibility would it be to do so? There are challenges, which I'll explain by looking at how the U.S. government and industry view academic research in this domain. In the realm of cyberresilience for energy systems, the DOE supports "the research, development and demonstration of new tools and technologies."[2] The expectations of the DHS are similar. The DOE in partnership with the DHS has been investing more than US$30 million during five years in two academic consortiums that perform translational research on cyberresilience for energy delivery systems—I'm the principal investigator for one of these consortiums. The DOE also invests significantly on transitional research led by industry and by national labs. Although the DOE and DHS missions address a clear need and their programs can point to a number of impactful outcomes, the emphasis does not easily accommodate any early-stage research needed before the idea of a tool is even possible.

My understanding of industry's view of academic research is the result of a requirement our DOE-funded consortiums have to create a plan for self-sufficiency—after the DOE support ends, industry is to take over funding of the research. Consequently, we have been developing a proposal for an NSF Industry University Cooperative Research Center (IUCRC.)

My understanding of industry's view of academic research is the result of a requirement our DOE-funded consortiums have to create a plan for self-sufficiency.

The academic research performed by an IUCRC is selected and paid for by industrial members, and the NSF contributes funding for administration of the center. The model has worked well in research areas where a number of industrial competitors agree to jointly support the development of open precompetitive research. Obviously, to be successful, an IUCRC has to develop a value proposition that resonates with potential members. Toward this end, the NSF runs IUCRC proposal bootcamps based on the NSF's Innovation Core (I-Corps) training program. One of the key I-Corps ideas is to formulate hypotheses about the IUCRC's value proposition, then test and refine those hypotheses through structured interviews with many potential members.

In our bootcamp, we conducted nearly 50 interviews. Some of those interviewed were from utilities that deliver electric power and/or natural gas, some represented groups of such utilities, some were from manufacturers of devices used in energy systems, some were cybersecurity service providers, and some were consultants. What we learned was consistent with what we'd heard from industry people throughout the life of the DOE project. More than 90% of those interviewed said their company's primary value from engaging with academia is workforce development, writ large. The process of meeting students, recruiting interns, and eventually hiring new employees was identified as a strong value proposition, across all customer groups.

Development of existing employees by attendance at center-organized meetings was also widely valued, particularly to the utilities and consultants. At these events, people from both academia and industry can share their knowledge about emerging threats, active research, emerging technologies, and applicable software tools; we heard that industry attendees like to become more knowledgeable and return home to do their own jobs better. Responders also saw value in meetings where utilities, manufacturers, government agencies, and regulators can come together on neutral ground for open and frank discussions. Only fourth down the list of rank-ordered value propositions did we find access to software that results from center research.

One needs to interpret these results carefully. It is safe to say that industry values what academia can provide in terms of a hiring pool and what academia can teach it. The comparatively low score on research products must be viewed in the context of the question, "what is the value to you of directly interacting with an academic center?" and not "what is the value to you of commercial products whose provenance includes university research?" In particular, the results are not a refutation of the DOE/DHS's investment in academic research that transitions. The results do imply, though, that this particular industry would rather spend its own money on academically provided education than on academically provided as-yet-to-be-transitioned research results. On the face of it, many members of this industry will need some convincing to invest their own resources in academic research within an IUCRC framework.

I'm emphasizing early-stage research because it's what academics do best, and I think they have an underutilized role in the cyberdefense of critical infrastructures. The intellectual challenges tend to be of most interest to academics because there is a greater emphasis on ideas and less on implementation. Furthermore, academic advancement is in part a function of publications. The leading conferences and journals for cybersecurity research strongly favor early-stage ideas. Although development is key to transitional research, it takes more time and money to get publishable results than does early-stage work. Students need to publish to graduate and get jobs, and faculty need to publish to get tenure and, later, promotions. Early-stage research is a more efficient means toward publication.

To review the situation, early-stage research is needed to prime the pump for transitional research; however, the stakeholders responsible for critical infrastructure aren't investing significantly in it at universities. In the specific area of cybersecurity for critical infrastructure, the NSF will fund early-stage research and the DOE/DHS will fund transitional research, but the funding of early-stage research has been very small. This particular industry is interested in hiring students and in being educated by academia but ranks those interests higher than funding research itself. Finally, from the academic point of view, early-stage research is the sweet spot for its participation in addressing critical infrastructure vulnerabilities. That said, to choose relevant research problems in a particular application domain, the researchers have to understand the special characteristics of that domain, e.g., limitations on processing power and memory, the need for provably bounded end-to-end communication delays, and the characteristics of specialized devices that appear in the domain but not elsewhere. To be relevant, the researchers have to invest in learning about cyberrequirements of the domain, and research funding enables that learning.

There is, I think, a way forward, if government funding agencies were to see the value of using academia to help industry do a better job of protecting critical infrastructures. I can imagine a program by the NSF, DOE, or DHS that creates academic centers for specific domains, e.g., one on energy delivery systems, where the emphasis is on educating industry on best practices, keeping it informed of commercially available state-of-the-art security controls, and on soon-to-emerge technology to improve cybersecurity. Such a center might include training and workforce development courses, faculty/student visitations to industrial sites, internships, information webinars, white papers, meetings focused on addressing critical emerging issues, and multistakeholder semiannual meetings. But if there is value in having cybersecurity researchers participating—and I think this is essential—to draw them in and increase the number of students knowledgeable enough to join the industry, the center needs also to fund research projects, many of them early stage. The researchers need the exposure to industry to understand the specialized requirements of computing and communication in their domain and so identify research problems that are relevant. They need the feedback from industry on whether they understand the issues correctly. Industry needs the researchers for their knowledge, perspectives, and access to students.

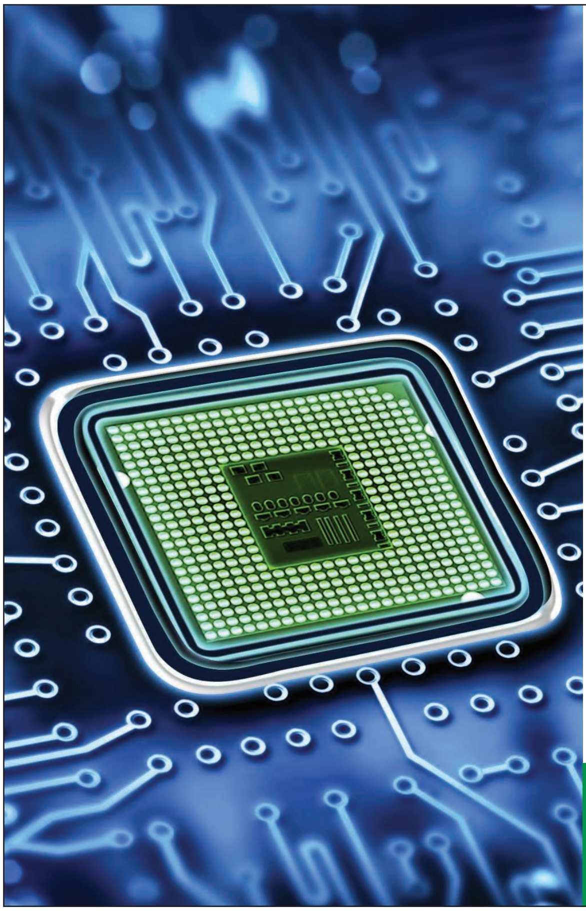
Centers like this could simultaneously address multiple needs:

- develop the domain-relevant early-stage results needed to launch research that transitions to practice
- increase the pool of students trained in cybersecurity within a critical infrastructure, for workforce development in both industry and academia
- provide cybersecurity training and advice to the small and medium-sized companies that cannot afford it otherwise
- keep larger companies apprised of the dynamically changing threat landscape and informed about leading-edge means of mitigating those threats.

For this idea to become reality, everyone has to bend a little. The government view of what it will fund with respect to industry/academia interaction needs to broaden. Industry needs to see that early-stage research can be leveraged to aid its workforce development needs. Academics need to accept the responsibility for outreach to industry as a condition for accepting research funding, embrace the need to understand the specialized requirements of the industry, and prioritize research areas to ones that are relevant to the industry. My experience with members of all of these groups is that many see the seriousness of critical infrastructure vulnerabilities and want to help, and I believe this willingness can lead to new ways of addressing the issue. ■

References

1. A. Flexner, "The usefulness of useless knowledge," in *The Usefulness of Useless Knowledge.* Princeton, NJ: Princeton Univ. Press, 2017, pp. 49–88.
2. Office of Cybersecurity, Energy Security, and Emergency Response, "Cybersecurity for critical energy infrastructure," 2019. [Online]. Available: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure



Digital Object Identifier 10.1109/MSEC.2019.2962590