DOI:10.1145/1646353.1646365

Douglas Maughan

Inside Risks
The Need for a National Cybersecurity Research and Development Agenda

Government-funded initiatives, in cooperation with private-sector partners in key technology areas, are fundamental to cybersecurity technical transformation.

Communications' *Inside Risks columns over the past two decades have frequently been concerned with trustworthiness of computer-communication systems and the applications built upon them. This column considers what is needed to attain new progress toward avoiding the risks that have prevailed in the past as a U.S. national cybersecurity R&D agenda is being developed. Although the author writes from the perspective of someone deeply involved in research and development of trustworthy systems in the U.S. Department of Homeland Security, what is described here is applicable much more universally. The risks of not doing what is described here are very significant.*

—Peter G. Neumann

President Barack Obama greets White House Cyber Security Chief Howard A. Schmidt, who was appointed in December 2009.

OFFICIAL WHITE HOUSE PHOTO BY LAWRENCE JACKSON

CYBERSPACE IS THE complex, dynamic, globally interconnected digital and information infrastructure that underpins every facet of society and provides critical support for our personal communication, economy, civil infrastructure, public safety, and national security. Just as our dependence on cyberspace is deep, so too must be our trust in cyberspace, and we must provide technical and policy solutions that enable four critical aspects of trustworthy cyberspace: security, reliability, privacy, and usability.

The U.S. and the world at large are currently at a significant decision point. We must continue to defend our existing systems and networks. At the same time, we must attempt to be ahead of our adversaries, and ensure future generations of technology will position us to better protect critical infrastructures and respond to attacks from adversaries. Government-funded research and development must play an increasing role toward achieving this goal of national and economic security.

Background

On January 8, 2008, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 formalized the Comprehensive National Cybersecurity Initiative (CNCI) and a series of continuous efforts designed to establish a frontline defense (reducing current vulnerabilities and preventing intrusions), which will protect against the full spectrum of threats by using intelligence and strengthening supply chain security, and shaping the future environment by enhancing our research, development, and education, as well as investing in "leap-ahead" technologies.

No single federal agency "owns" the issue of cybersecurity. In fact, the federal government does not uniquely own cybersecurity. It is a national and global challenge with far-reaching consequences that requires a cooperative, comprehensive effort across the public and private sectors. However, as it has done historically, the U.S. government R&D community, working in close cooperation with private-sector partners in key technology areas, can jump-start the necessary fundamental technical transformation.

Partnerships

The federal government must reenergize two key partnerships to successfully secure the future cyberspace: the partnership with the educational system and the partnership with the private sector. The Taulbee Survey[2] has shown that our current educational system is not producing the cyberspace workers of the future and the current public-private partnerships are inadequate for taking R&D results and deploying them across the global infrastructure.

Education. A serious, long-term problem with ramifications for national security and economic growth is looming: there are not enough U.S. citizens with computer science (CS) and science, technology, engineering, and mathematics (STEM) degrees being produced. The decline in CS enrollments and degrees is most acute. The decline in undergraduate CS degrees portends the decline in master's and doctoral degrees as well. Enrollments in major university CS departments have fallen sharply in the last few years, while the demand for computer scientists and software engineers is high and growing. The Taulbee Survey[2] confirmed that CS (including computer engineering) enrollments are down 50% from only five years ago, a precipitous drop by any measure. Since CS degrees are a subset of the overall requirement for STEM degrees and show the most significant downturn, CS degree production can be considered a bellwether to the overall condition and trend of STEM education. The problems with other STEM degrees are equally disconcerting and require immediate and effective action. At the same time, STEM jobs are growing, and CS jobs are growing faster than the national average.

At a time when the U.S. experiences cyberattacks daily and as global competition continues to increase, the U.S. cannot afford continued ineffective educational measures and programs. Revitalizing educational systems can take years before results are seen. As part of an overall national cybersecurity R&D agenda, the U.S. must incite an extraordinary shift in the number of students in STEM education quickly to avoid a serious shortage of computer scientists, engineers, and technologists in the decades to come.

Public-Private Partnerships. Information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing cybersecurity issues requires public-private partnerships as well as international cooperation. The public and private sector interests are dependent on each other and share a responsibility for ensuring a secure, reliable infrastructure. As the federal government moves forward to enhance its partnerships with the private sector, research and development must be included in the discussion. More and more private-sector R&D is falling by the wayside and, therefore, it is even more important that government-funded R&D can make its way to the private sector, given it designs, builds, owns, and operates most of the critical infrastructures.

Technical Agenda

Over the past decade there have been a significant number of R&D agendas published by various academic and industry groups, and government departments and agencies (these documents can be found online at http://www.cyber.st.dhs.gov/documents.html). A 2006 federal R&D plan identified at least eight areas of interest with over 50 project topics that were either being funded or should be funded by federal R&D entities. Many of these topic areas have been on the various lists for over a decade. Why? Because the U.S. has underinvested in these R&D areas, both within the government and private R&D communities.

The current public-private partnerships are inadequate for taking R&D results and deploying them across the global infrastructure.

The Comprehensive National Cyber Initiative (CNCI) and the President's Cyberspace Policy Review[3] challenged the federal networks and IT research community to figure out how to "change the game" to address these technical issues. Over the past year, through the National Cyber Leap Year (NCLY) Summit and a wide range of other activities, the U.S. government research community sought to elicit the best ideas from the research and technology community. The vision of the CNCI research community over the next 10 years is to "transform the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances."

The leap-ahead strategy aligns with the consensus of the U.S. networking and cybersecurity research communities: That the only long-term solution to the vulnerabilities of today's networking and information technologies is to ensure that future generations of these technologies are designed with security built in from the ground up. Federal agencies with mission-critical needs for increased cybersecurity, which includes information assurance as well as network and system security, can play a direct role in determining research priorities and assessing emerging technology prototypes.

The Department of Homeland Security Science and Technology Directorate has published its own roadmap in an effort to provide more R&D direction for the community. The Cybersecurity Research Roadmap[1] addresses a broad R&D agenda that is required to enable production of the technologies that will protect future information systems and networks. The document provides detailed research and development agendas relating to 11 hard problem areas in cybersecurity, for use by agencies of the U.S. government. The research topics in this roadmap, however, are relevant not just to the governments, but also to the private sector and anyone else funding or performing R&D.

While progress in any of the areas identified in the reports noted previously would be valuable, I believe the "top 10" list consists of the following (with short rationale included):

1. Software Assurance: poorly written software is at the root of all of our security problems;
2. Metrics: we cannot measure our systems, thus we cannot manage them;
3. Usable Security: information security technologies have not been deployed because they are not easily usable;
4. Identity Management: the ability to know who you are communicating with will help eliminate many of today's online problems, including attribution;
5. Malware: today's problems continue because of a lack of dealing with malicious software and its perpetrators;
6. Insider Threat: one of the biggest threats to all sectors that has not been adequately addressed;
7. Hardware Security: today's computing systems can be improved with new thinking about the next generation of hardware built from the start with security in mind;
8. Data Provenance: data has the most value, yet we have no mechanisms to know what has happened to data from its inception;
9. Trustworthy Systems: current systems are unable to provide assurances of correct operation to include resiliency; and
10. Cyber Economics: we do not understand the economics behind cybersecurity for either the good guy or the bad guy.

Life Cycle of Innovation

R&D programs, including cybersecurity R&D, consistently have difficulty in taking the research through a path of development, testing, evaluation, and transition into operational environments. Past experience shows that transition plans developed and applied early in the life cycle of the research program, with probable transition paths for the research product, are effective in achieving successful transfer from research to application and use. It is equally important, however, to acknowledge that these plans are subject to change and must be reviewed often. It is also important to note that different technologies are better suited for different technology transition paths and in some instances the choice of the transition path will mean success or failure for the ultimate product. There are guiding principles for transitioning research products. These principles involve lessons learned about the effects of time/schedule, budgets, customer or end-user participation, demonstrations, testing and evaluation, product partnerships, and other factors.

In order to achieve the full results of R&D, technology transfer needs to be a key consideration for all R&D investments.

A July 2007 U.S. Department of Defense Report to Congress on Technology Transition noted there is evidence that a chasm exists between the DoD S&T communities and acquisition of a system prototype demonstration in an operational environment. DOD is not the only government agency that struggles with technology transition. That chasm, commonly referred to as the "valley of death," can be bridged only through cooperative efforts and investments by both research and acquisition communities.

There are at least five canonical transition paths for research funded by the federal government. These transition paths are affected by the nature of the technology, the intended end user, participants in the research program, and other external circumstances. Success in research product transition is often accomplished by the dedication of the program manager through opportunistic channels of demonstration, partnering, and sometimes good fortune. However, no single approach is more effective than a proactive technology champion who is allowed the freedom to seek potential utilization of the research product. The five canonical transition paths are:

- Department/Agency direct to Acquisition
- Department/Agency to Government Lab
- Department/Agency to Industry
- Department/Agency to Academia to Industry
- Department/Agency to Open Source Community

In order to achieve the full results of R&D, technology transfer needs to be a key consideration for all R&D investments. This requires the federal government to move past working models where most R&D programs support only limited operational evaluations and experiments. In these old working models, most R&D program managers consider their job done with final reports, and most research performers consider their job done with publications. In order to move forward, government-funded R&D activities must focus on the real goal: technology transfer, which follows transition. Current R&D principal investigators (PIs) and program managers (PMs) aren't rewarded for technology transfer. Academic PIs are rewarded for publications, not technology transfer. The government R&D community must reward government program managers and PIs for transition progress.

Conclusion

As noted in the White House Cyberspace Policy Review,[3] an updated national strategy for securing cyberspace is needed. Research and development must be a full partner in that discussion. It is only through innovation creation that the U.S. can regain its position as a leader in cyberspace.

References

1. A Roadmap for Cybersecurity Research, Department of Homeland Security Science and Technology Directorate, November 2009; http://www.cyber.st.dhs.gov/documents.html
2. Taulbee Survey 2006–2007, Computing Research News 20, 3. *Computer Research Association*, May 2008.
3. White House Cyberspace Policy Review; http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_review_final.pdf

Douglas Maughan (Douglas.Maughan@dhs.gov) is a program manager for cybersecurity R&D at the U.S. Department of Homeland Security in Washington, D.C.