COMPUTING RESEARCH ASSOCIATION

CRA

# TESTIMONY OF THE<br>COMPUTING RESEARCH ASSOCIATION<br>FOR<br>THE PITAC CYBER SECURITY SUBCOMMITTEE<br>TOWN HALL MEETING ON CYBER SECURITY<br>RESEARCH AND DEVELOPMENT

**July 29, 2004**

Thank you Chairman Leighton and other members of the PITAC Subcommittee on Cyber Security for this opportunity to provide input to the committee's efforts to review the Nation's cyber security research and development enterprise. The Computing Research Association (CRA), an organization representing more than 200 North American academic departments of computer science, computer engineering and related fields; 23 laboratories and centers in industry, government, and academia engaging in basic computing research; and 6 affiliated professional societies, has great interest in the current state of federally-supported cyber security research and development activities, and a few concerns.

As the National Research Council noted in its 2002 report *Making the Nation Safer*, information technology constitutes the "control loop" of essentially every aspect of our critical national infrastructure – the electric power grid, the financial grid, the telecommunications grid, the food distribution network – "[making] the computers and communications systems of the nation a critical infrastructure in and of themselves." In that report, the NRC concluded that the most significant long-term step the Federal government could take to protect this information infrastructure was a sustained commitment to IT research and development, specifically in the areas of information and network security, new IT for emergency response, and new IT for detection, prevention, remediation and attribution of attacks.

The NRC report delineated a number of research areas in five broad categories important to the goal of protecting the information infrastructure: improved information and networking security; command, control, communications and information (C3I) for emergency response; information fusion; privacy and confidentiality; and planning for the future. The list is well-conceived and we commend it to the attention of the committee. Just as significantly, the panel identified a number of important attributes the federal investment in cyber security research and development should posses. Federally-supported research, the panel concluded, should:

- Engage and support multidisciplinary, problem-oriented research useful to both civilian and military users.
- Have a research program driven by a deep understanding of vulnerabilities. This will likely require access to classified information, even though most of the research will be unclassified.
- Support a substantial effort in research areas with a long time horizon for payoff, with recognition that such investigations have been housed most often in academia.
- Provide support extending for time scales that are long enough to make meaningful progress on hard problems and in sufficient amounts that reasonably operating environments for the technology could be constructed.
- Invest some small fraction of its budget on thinking "outside the box" in consideration (and possible creation) of alternative futures.

- Be more tolerant of research directions that appear not to promise immediate applicability.
- Be overseen by a board or other entity with sufficient stature to attract top talent, provide useful feedback, and be an effective sounding board for that talent.
- Pay attention to the human resources needed to sustain the counterterrorism information technology research agenda – noting that only a very small fraction of the nation's graduating doctoral students in information technology specialize in information and network security or emergency communications, very few professors conduct research in these areas, and only a very few universities support research programs in these fields. [1]

CRA's most serious concern with the current state of Federal support for cyber security R&D, particularly research supported by two key mission agencies – the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS) – is that it lacks a significant number of the key attributes identified by the NRC. We are concerned that the federal effort is under-funded and poorly balanced between short and long-term efforts. Additionally, we are concerned that current law has a chilling effect on some research efforts in cyber security, and that current agency policies at odds with the attributes cited above appear to be driving university-based researchers away from research funded by critical mission agencies.

## The problem of funding and focus

As the committee is aware, DHS has described its research efforts in cyber security as necessarily short-term in emphasis. Simon Szykman, Director of Cyber Security R&D at DHS testified before PITAC on April 13, 2004, that the agency will continue to focus its research agenda on the "low-hanging fruit" – technologies that are almost ready for deployment – for at least the next "couple of years" in an effort to get as many of these new technologies into the field as quickly as possible. For now, Szykman (and Amit Yoran, DHS' Director of the National Cyber Security Division, who also testified) said, DHS will be dependent on the work of agencies like the National Science Foundation (NSF) and DARPA for long-range research that underpins their short-term efforts.

While this approach is arguably appropriate for DHS to pursue in the short-term, we have concerns with its application in the current environment. First, NSF and DARPA both have issues of their own regarding long-term cyber-security funding. For NSF, the issue is primarily one of funding. As Carl Landwehr, Program Director for NSF's Cyber Trust initiative, testified at the April 2004 PITAC meeting, the agency receives far more good proposals for cyber security related topics than it could possibly fund with its current appropriation. He cited a sobering example: the recent $30 million Cyber Trust solicitation generated over 230 "small" proposals, of which the agency can fund about 30; 125 "medium" proposals, of which the agency can fund 6 or 8; and 30 large scale proposals, of which just 1 or 2 might receive funding – a success rate of between 5 and

[1] National Research Council, 2002, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, Washington, DC.

10 percent. (Landwehr also noted that this low success rate was not unusual in NSF's Computing and Information Science and Engineering (CISE) directorate.) Of the proposals received, Landwehr estimated 25 percent would likely be ranked by NSF panels as good enough to fund if funds were available. Put another way, by this metric there are enough good ideas in the community to fuel 2.5 times the research than can currently be supported.

For DARPA, the issues are policy-related rather than funding-related (indeed, DARPA Director Anthony Tether noted during his testimony at the April PITAC meeting that he believed DARPA program managers were "idea starved, not money starved" when it came to funding cyber security research). CRA has been concerned for some time over what we see is a shift at the agency from a focus on long-term research to shorter-term research. Tether, since taking over as head of the agency in 2001, has been plain in his desire to reshape DARPA in the model of a high-tech venture capital firm – identifying promising technologies early and providing them with the capital needed to turn them into demonstrable technologies on short-timelines. Key to this identification process is DARPA's implementation of a formal "go/no-go" decision matrix for all DARPA funded research projects. In addition to facing a traditional annual review, in which DARPA managers verify that contract work is proceeding according to plan and on-budget, DARPA contract recipients now face multiple review milestones at relatively short 12 to 18 month intervals, by which their projects must deliver some demonstrable result in order to receive continued funding.

To some, DARPA's approach appears to represent a reasonably business-like approach to providing good stewardship over taxpayer dollars in the course of developing the technologies necessary for national security in the post-September 11th world. However, for university researchers accustomed to working on basic research problems, the idea of "scheduling" breakthroughs or demonstrable results on 12 month timelines is anathema to the basic research enterprise and nearly impossible to do in an academic environment. CRA believes that DARPA's new funding regime has constrained university researchers from pursuing DARPA contracts, effectively preventing some of the best minds in the country from working on national security problems. The "go/no-go" decisions result in research that is evolutionary, not revolutionary, with potential grantees only proposing ideas they can be sure to deliver significant progress on in 12 months. Failing to consider long-term research could leave the nation once-again "flat-footed" to the new threats of the 21st Century.[2]

[2] CRA took this issue to Congress in 2002 and received a sympathetic reception from members of Senate Armed Services Committee who put the question to Tether during his annual appearance before the committee as part of the Defense Authorization process. Tether brushed the concerns aside in his official response:

> I do not believe our "Go/No-Go" milestones will make our work less revolutionary nor do I think they will interfere with university participation in our programs. Instead, I view them as a technique for providing solid management and accountability for the significant investments we make with taxpayer dollars. … This technique allows progress to occur quickly and keeps everyone focused on accomplishing goals they can see happen yet that will still have a big long-

The other policy concern surrounding DARPA is the increased use of classification to limit the dissemination of its cyber security research underway. Tether has stated in a number of public forums – including at CRA's Computing Leadership Summit in February 2004 and the April 2004 meeting of PITAC – that the move towards increasing the amount of research under classification is justified given the Department of Defense's increasing reliance on "network-centric" operations for its warfighting capability. There are, of course, important reasons for classifying federal research, especially when it is clear that the research might reveal our capabilities or vulnerabilities. However, it should also be understood that there are real costs – including that the research is unavailable for public dissemination and scrutiny, and that many university researchers, arguably some of the best minds in the country, are no longer able to contribute to the work. In the case of DARPA's cyber security research, there is another significant cost to bear as well. The military (and the government overall) has a huge dependence on our nation's commercial infrastructure, but classifying the research in information security means that it is largely unavailable for use in protecting this commercial infrastructure.

In light of these issues at DARPA and the continued under-funding of NSF, CRA does not take much comfort in DHS' dependence upon these two agencies as the source of the long-term research so critical to the agency's long-term mission. Indeed, we believe it would be in the best interest of DHS – and, by extension, the nation – to nurture its own basic research capability in much the same way the Department of Defense did in creating DARPA more than 40 years ago. DARPA allowed DOD to look to the distant future to identify areas of research that might one day prove important to the DOD

> term impact. Industry understands this method because it is a technique used by the best industrial managers for executing a difficult multi-year contract.

The Committee remained unconvinced, however, and included an admonition to DARPA in the committee report accompanying FY 2003 Defense Authorization Act:

> The committee, however, is concerned about recent trends in the agency-sponsored research that appear more shortsighted in their approach, particularly the emphasis on 12- and 18-month reviews in order to attempt to eliminate non-promising technologies.
>
> The committee supports effective internal oversight and commends DARPA for pursuing truly innovative technologies. However, annual reviews may not be appropriate for all basic and applied defense-related research programs. Additionally, these reviews have a discouraging effect on the intended long-term payoff of the research and are especially inconsistent with the time frames and pace of university research. The committee is concerned that this near-term approach to basic and applied research will have detrimental consequences on the ability to develop innovative solutions to future threats. Therefore, the committee urges DARPA to re-evaluate its policies for reviewing and terminating awards in scientific and technical areas where the Department of Defense is dependent on DARPA's ability to do revolutionary research that requires some time to develop and mature.

The Committee followed that up with a requirement in the FY 2004 Defense Authorization Act that the National Academies of Science do a review of all Defense Basic Research, including a whether broad agency announcements permit truly innovative approaches to be proposed. That study is headed General Larry D. Welch of the Air Force Science and Technology Board and is ongoing.

mission, and then empowered program managers to place "big bets" in key areas and communities with the expectation that payoffs may be long in coming – and perhaps in unexpected areas. In the process, DARPA funding at universities helped develop and train the next generations of researchers. The resulting successes are well known. DARPA has been credited with between a third and a half of all the major innovations in computer science and technology. We are concerned that by focusing on short-term research, DHS may be losing an opportunity to capitalize on a similar approach with the agency's own Homeland Security Advanced Research Projects Agency (HSARPA).

We are also concerned about DHS' overall commitment to cyber security research. As the committee knows, out of a research and development budget of nearly $1 billion, DHS has invested less than 2 percent in cybersecurity R&D. Even this worryingly low level of investment was the result of Congressional and community outcry – DHS initially proposed less than 1 percent. CRA believes that DHS will only be able to make significant progress towards protecting the nation's information infrastructure in the short and long-term by funding research in cyber security at adequate levels.

In a general sense, it is critically important that we have a sustained commitment to funding long-term cyber security research from a diversity of agencies, with the acknowledgement that we cannot predict when (or if) the results of research will be applicable. Thus it is important that we invest now, in multiple efforts, and not prematurely judge the output. For good research to occur, we need some element of risk and uncertainty, and the support should be large enough and long enough to allow investigation of new ideas that may not have immediately obvious application.

**Chilling effects and the research pool**

In addition to funding and focus issues at the major funding agencies, we believe there are other issues constraining research in cyber security. One such issue is the chilling effect on research that can be the result of laws aimed at protecting intellectual property or privacy rights. Perhaps the best example of this is found in the controversy surrounding the Digital Millennium Copyright Act (DMCA), enacted in 1998.

The DMCA attempts to protect copyrighted digital content by prohibiting the circumvention of any copyright enforcing technologies (watermarks, encrypted content, or warning stickers, for example). CRA, along with a number of other computing societies, has argued that the DMCA's overly broad approach to anti-circumvention puts computer security researchers at risk of running afoul of the law in the course of their normal work. The U.S. Public Policy Committee of the Association for Computing Machinery (USACM), a CRA affiliate organization, notes

> [T]he "anti-circumvention provisions" of the DMCA interfere with many legal, non-infringing uses of digital computing and prevent scientists and technologists from circumventing access technologies to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, to analyze and stop malicious code (e.g., viruses), and to conduct forms of

> desired educational activities. In some instances, the threat of legal action under the DMCA has deterred scientists from publishing scholarly work or even publicly discussing their research, both fundamental tenets of scientific discourse.

CRA joins with USACM and other stakeholders in the research community in recommending that the anti-circumvention provisions of the DMCA be revised to restrict only circumvention directly involved in copyright infringement.

Finally, as the NRC noted, the current pool of researchers in industry and academia with information security degrees is still relatively small. Federal support for university-based cyber security research is the primary driver for increasing the size of that pool. But such support can only be effective, can only attract new faculty and graduate students to the area, if it is sustained.

We firmly believe that the nation cannot hope to protect its information infrastructure without a sustained commitment to cyber security research and development and a review of some of the policies that artificially constrain that research. As PITAC pointed out the 1999 report *Investing in Our Future*, the relatively modest overall federal IT R&D investment has paid enormous dividends – changing our lives, driving our economy, and transforming the conduct of science. We believe an investment in cyber security R&D will net similar returns.

*The Computing Research Association (CRA) is an association of more than 200 North American academic departments of computer science, computer engineering, and related fields; laboratories and centers in industry, government, and academia engaging in basic computing research; and affiliated professional societies.*

*CRA's mission is to strengthen research and education in the computing fields, expand opportunities for women and minorities, and improve public and policymaker understanding of the importance of computing and computing research in our society.*

*For more information, please see the CRA website at: http://www.cra.org*