

July 7, 2005

Chairman Sherwood Boehlert
Committee on Science
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Boehlert:

I have enclosed responses to your written questions following the May 12, 2005 hearing on "The Future of Computer Science Research in the U.S.". Also included are my responses to written questions submitted by Ranking Member Gordon and Representative Jackson Lee.

As I stated in my testimony, the challenges we face with cyber security research are similar to those we face with IT at large. In particular, there is much research that urgently needs to be done, little of which will be funded by industry. It is important that the Federal Government take action before the situation worsens and the cost of inaction becomes even greater.

Thank you for the opportunity to supply testimony on this important topic.

Sincerely,

Dr. Tom Leighton
Chief Scientist and Co-Founder
Akamai Technologies, Inc.

Questions from Science Committee Chairman Sherwood Boehlert:

Question One:

What kind of computer science research isn't DARPA supporting that you think it should? Is it just a matter of more funding or are there programs that are of a lower priority that should be cut?

Answer:

I am most concerned by DARPA's reduction of support for university-led research in computer science. This is not a problem limited to a particular research area within the discipline per se. Rather, it is a trend across the spectrum of computer science. While there may be examples of areas, such as the cognitive computing effort mentioned during the hearing, where DARPA is still funding basic research in computer science, university funding has been greatly reduced or eliminated in many important areas.

The Defense Science Board noted this trend in February 2005 in their examination of DOD's efforts to maintain an adequate supply of High Performance Microprocessors (incidentally, an area in which DSB concluded DOD -- primarily DARPA -- was "no longer seriously involved in...research to enable the embedded processing proficiency on which its strategic advantage depends"). The DSB recognized the crucial payoff gained by DOD -- and ultimately the nation -- from DARPA's prior significant involvement in university-led IT R&D:

"From the early 1960's through the 1980's, one tremendously successful aspect of the DOD's funding in the information technology space came from DARPA's unique approach to the funding of Applied Research (6.2 funding), which hybridized university and industry research through a process that envisioned revolutionary new capabilities, identified barriers to their realization, focused the best minds in the field on new approaches to overcome those barriers and fostered rapid commercialization and DOD adoption. The hybridization of university and industry researchers was a crucial element; it kept the best and the brightest in the university sector well informed of defense issues and the university researchers acted as useful 'prods' to the defense contractors, making it impossible for them to dismiss revolutionary concepts whose feasibility was demonstrated by university-based 6.2 efforts that produced convincing 'proof of concept' prototypes.

Recently, DARPA has further limited university participation, especially as prime contractors, in its Computer Science 6.2 programs, which were by far its most significant investments in university research (vastly outstripping 6.1 funding). These limitations have come in a number of ways, including non-fiscal limitations, such as the classification of work in areas that were previously unclassified, precluding university

submission as prime contractors on certain solicitations, and reducing the periods of performance to 18-24 months.”

For FY 2005, DARPA reported to the National Coordination Office for IT Research and Development that it planned to make *no* investment in the High Confidence Software and Systems research area. This area includes several important topics, such as cyber security R&D.

As Director Tether’s testimony before the Committee indicated, DARPA is funding *classified* research efforts in the cyber security space. Because the work is classified, however, the amount and nature of the work can’t be shown in the NCO’s budget supplement. More importantly, the university research community is largely unable to participate in the research, and constraints on the dissemination of the results of the work limit the community’s ability to drive further innovation based on it.

In its March 2005 review of federal cyber security R&D, the President’s Information Technology Advisory Committee (PITAC) noted that this trend stands to disadvantage both the civilian and military sectors. As an example, PITAC cited the potential impact of the increased use of classification on DOD’s planned Global Information Grid (GIG) - - a multilayered network to link weapons, intelligence, and military personnel for “network enhanced” warfare:

“The Defense Department intends the most sensitive portions of the GIG to be self-contained, reducing the military’s potential exposure to the insecurities associated with the public IT infrastructure. However, some less sensitive portions of the GIG are expected to connect to the Internet, at least part of the time. Vulnerabilities are introduced whenever highly sensitive defense networks and civilian networks intersect, giving both communities a significant stake in cooperating to improve the security of the civilian IT infrastructure. Also, economic realities dictate that today’s military networks and tomorrow’s GIG use civilian commercial hardware and software, exposing those networks to the security vulnerabilities of such products. Thus, the success of the GIG as a secure IT infrastructure of the future – and the near-term success of today’s military networks – depends in part on improvements in the security of the civilian IT infrastructure. Yet because the civilian R&D community has access only to the results of unclassified research, reduced support for this community will have a harmful impact on its ability to generate the fundamental discoveries upon which future generations of security products and practices will be based.”

PITAC identified 10 specific priority areas, listed below, in computer science of “paramount importance” to securing the national IT infrastructure. DARPA’s support for unclassified research in these areas would likely prove enormously beneficial to DOD and the nation:

1. Authentication Technologies
2. Secure Fundamental Protocols

3. Secure Software Engineering and Software Assurance
4. Holistic System Security
5. Monitoring and Detection
6. Mitigation and Recovery Methodologies
7. Cyber Forensics
8. Modeling and Testbeds for New Technologies
9. Metrics, Benchmarks and Best Practices
10. Research into Human and Organizational Aspects of IT Infrastructures.

There are other areas in which DARPA's efforts are under supported (or absent completely). DARPA's unclassified efforts in Software Design and Productivity, for example, have also been discontinued, according to the FY 2005 plan and FY 2006 request. Low power computation models, improved mesh & grid computing methods, easy-to-learn and use HCI, fault tolerance and replication for portable computing, and federated database management and integration, are all example areas of computing research where advances could help the warfighter, as well as the civilian population, homeland defense and the economy.

DARPA's mission is to support the warfighter and DOD future needs. DARPA research has, in the past, often met those needs by "pushing the envelope" such that advances were adopted in the civilian sphere, thus making them available in quantity, and at lower cost, to the military as "commodity" computing items. By not pursuing research in this realm, or by classifying it, the commoditization and the synergy produced by mixing both university and industrial talent, are missing.

But as the DSB report alluded, DARPA's key role in promoting innovation in IT -- innovation that has honed America's war fighting capability, fueled the new economy, and revolutionized health care and the conduct of the sciences -- wasn't just its support for particular research areas. It was its unique approach (and commitment) to developing communities of researchers in both industry and academia focused on problems in computer science. DARPA continues to maintain a focus on some of those important problems, but its growing failure to support the university elements of that community is altering the innovation ecosystem in an increasingly negative way. And worse yet, no other mission agency has yet picked up the mantle, leaving NSF to bear the bulk of support for university-led fundamental computer science research.

In summary, I do not believe that the problem necessarily results from a lack of money, but rather from a change in prioritization. Whereas overall funding for computer science

has increased over the last several years at DARPA, DARPA funding for basic research at universities in computer science has dropped significantly.

Question Two:

At the hearing, Dr. Tether mentioned several times his agency's work on cognitive computing as an example of long-range research underway at DARPA. Is that the kind of long-range computer science research that you believe DARPA should be doing? Why or why not?

Answer:

I am not directly familiar with DARPA's program in cognitive computing, but I do believe that research in this area is worthwhile. However, it is only one area of computer science and will not address many needs of the warfighter and the nation. For example, research in this area will probably not be relevant to the area of cyber security.

Question Three:

What criteria should we be using to determine if federal support for fundamental research in computer science in general and cyber security in particular is adequate?

Answer:

"How much should we spend?" is always a difficult question when it comes to funding basic research. The reason is that the benefit derived from the research generally is not realized until many years later. And, basic research is a high-risk endeavor. Not every idea pans out. Indeed, fundamental research, by its very nature, should be expected to have many failures. Risk-averse research simply does not lead to fundamentally new ways of thinking or to breakthroughs in the most important problems.

That said, there are measures that one can use to determine if the levels of funding are inadequate. First, the success rates of qualified grant proposals can be examined and compared across disciplines. As was noted in prior testimony, the success rate of qualified proposals in computer science at NSF lags far behind the NSF-wide average. The success rate in the area of cyber security is even smaller, a factor of three smaller than the NSF-wide average. These statistics indicate that there is good research that is going unfunded in computer science and that the lack of funding in computer science is out of proportion with other disciplines.

Second, one can look at the historical return on investment for research expenditures in a particular field. As was noted in prior testimony, the return on investment for academic computer science research over the last several decades has been extraordinary. Not only has the research led to the creation of numerous billion-dollar industries, but it has led, in part, to our Nation's pre-eminence in technology as a whole. If history is any guide, we

should be spending far greater sums on fundamental research in computer science than we do today.

Third, one can turn to experts for advice. PITAC was one such body of experts in information technology and they have made it very clear that our underinvestment in basic cyber security research poses a significant threat to our national well being. PITAC had planned to study the adequacy of our overall investment in IT R&D but their term has expired and no renewals have been announced.

Questions from Ranking Member Gordon:

Question One:

What efforts are now being made and what mechanisms exist to transition the results of federally funded cyber security research to commercial products and methods, and do you have recommendations for additional federal efforts in this area?

Answer:

As was noted in the PITAC report “Cyber Security: A Crisis of Prioritization”, “current cyber security technology transfer efforts are not adequate to successfully transition Federal research investments into civilian sector best practices and products.”

PITAC recommended that “the Federal government should strengthen its cyber security technology transfer partnership with the private sector. Specifically, the Federal government should place greater emphasis on the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated; jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results are showcased; fund technology transfer efforts (in cooperation with industry) by researchers who have developed promising ideas or technologies; and encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.”

In its discussion, PITAC noted that “technology transfer enables the results of Federally supported R&D to be incorporated into products that are available for general use. There has been a long and successful history of Federally funded IT R&D being transferred into products and best practices that are widely adopted in the private sector.”

“The diffusion of Federally supported IT R&D into products and practices benefits both consumers and developers:

- Consumers have benefited from faster hardware, faster networks, better software that is easier to use, and more frequent time- and labor-saving upgrades.
- IT research often results in new ideas and prototypes that can be rapidly developed into new or improved commercial products. The developers of such innovations are free to carry their innovative ideas into the marketplace, benefiting all consumers.”

“Unlike other IT products, cyber security’s benefits are measured by the absence of problems in IT systems. Because the market for these benefits has historically been small, interest is limited among both start-ups and large companies.”

PITAC believes that, “given the value and difficulty of technology transfer, the Federal government should support programs to transform existing and future cyber security research results into commercial products or operational best practices. Specifically, the Federal government should:

- Strengthen the development of metrics, models, datasets, and testbeds so that new products and best practices can be evaluated.
- Jointly sponsor with the private sector an annual interagency conference at which new cyber security R&D results, especially those conducted or sponsored by the Federal government, are showcased.
- Require grant proposals to describe the potential practical utility of their research results and have the coordinating body identified in Recommendation 4 of the PITAC report collect and publish these descriptions. (While fundamental research is usually undertaken without any direct transition path envisioned, cyber security research is often undertaken in the context of recognized problems, and documenting logical connections with real world problems is worthwhile.)
- Establish a fund to support technology transfer efforts by researchers who have developed promising ideas or technologies. This fund could also help researchers cooperate with industry to bring products or enhancements rapidly to market.
- Establish and maintain a national database of results from Federally funded cyber security research, allowing vendors to identify ideas that can be incorporated into commercial products.
- Encourage Federally supported graduate students and postdoctoral researchers to gain experience in industry as researchers, interns, or consultants.
- Encourage agency investment in technology transfer of cyber security R&D results through the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs of the Federal government.

“The Federal government and the private sector, by working together, can effectively and efficiently transfer Federally funded cyber security research results into commercial products and build an innovative cyber security workforce, and by doing so can help our society realize the potential benefits of this research.”

Question Two:

The President’s Information Technology Advisory Committee report on cyber security finds that the academic research community in cyber security research is below critical mass.

- a) To what extent would this be corrected simply by increasing the amount of research funding available?
- b) Are there other impediments to bringing more researchers to this field aside from the availability of research funding?

Answer:

As PITAC notes in its report, increasing the level of funding for basic research in cyber security is required to increase the size of the academic research community in cyber security. But it is not sufficient. The long term stability of the funding is also important, and it is critical that the university research not be classified.

I do not mean to imply that all cyber security research should be unclassified. Indeed, classified research in the area of cyber security is certainly a worthwhile endeavor. However, if most or all research in cyber security is classified, then university researchers (with whom much of our Nation's networking and computer science expertise resides) will not be able to contribute to the discovery of the breakthroughs that are so badly needed in this area. Moreover, the technology transfer needed to convert breakthroughs into products and best practices will also be seriously impeded.

Questions from Representative Jackson Lee:

Question One:

While I am unsatisfied by the status of computer science research being conducted on the federal level, I am also disturbed by the lack of female and minority representation in the field of computer science. The statistics show that women and minorities are not being proportionally represented in academia when it comes to computer science. In 2003, women represented barely over 20% of the computer science doctoral degrees granted. The same statistics show that in 2003, the White population made up about 70% of the doctoral degrees granted to U.S. citizens and permanent residents. At the same time, Asian/Pacific Islanders made up about 20% of the doctoral degrees granted, but Blacks, Hispanics, and American Indian/Native Alaskans made up less than 5% of the doctoral degrees granted. These statistics are very discouraging and show that we are not reaching out to our entire population. Indeed, the problem starts in the classroom, where many under-privileged youth do not have nearly the same access to computers and the Internet. If they don't have this background at an early age, its not surprising that they don't pursue the field in higher education and later in life. What are we doing to reach women, minorities, and the under-privileged in our society?

Answer:

I do not have sufficient expertise to provide an answer to this question. That said, I am painfully aware of lack of female and minority representation in the field of computer science (as well as related fields such as mathematics).

Question Two:

Your committee's report on cyber security recommends an increase to NSF's budget for cyber security research to \$90 million per year and "substantial" increases in civilian cyber security R&D at DARPA and the Department of Homeland Security.

- a) Why is there a recommendation for a specific increase for NSF, but not for the other agencies?
- b) Did your committee consider the need for funding increases at NIST or other federal agencies?

Answer:

NSF is the only agency for which we had enough credible data on research funding in order to make a specific recommendation for funding levels. That said, a comparable amount of funding for basic non-classified research at DARPA and DHS would certainly be in the Nation's interest. As was noted in prior testimony, DARPA has shifted a significant amount of funding away from universities in cyber security in favor of more directed and/or classified work, and DHS (which is tasked with the Nation's cyber security) spends only a tiny fraction of its large S&T budget on cyber security.

NIST, NIJ, DHS, DOE and other agencies should all re-examine the role they play in cyber security research. Increases in funding at all of them is probably in the Nation's best interest.

However, without better data, a clear understanding of how the money would be spent at those agencies, and some kind of national strategy, the committee was unable to formulate specific recommendations -- especially at a time when there are such large Federal deficits.