Testimony
House Committee on Science and Technology
"Networking and Information Technology Research and Development"
Amit Yoran
NetWitness Corporation
April 1, 2009

Mr. Chairman and Ranking Member, thank you for the opportunity to testify before the House Committee on Science and Technology on "Networking and Information Technology Research and Development."

My name is Amit Yoran and I am the CEO of the NetWitness Corporation, a company providing next generation cybersecurity monitoring technologies to the US Government and the private sector, and in delivering critical infrastructure cyber protection to the Nation. I also serve as a member of the CSIS Cyber Commission advising the 44th Presidency and on numerous security industry advisory bodies.

I have served as the first Director of the National Cyber Security Division (NCSD) in standing up the United States Computer Emergency Readiness Team (US-CERT) and Einstein program at the Department of Homeland Security (DHS), as CEO and advisor to In-Q-Tel, as founder and CEO of Riptech, an innovative cyber security company, and as manager of the Vulnerability Analysis Program (VAP) of the US Department of Defense's Computer Emergency Response Team (DoD CERT). I received a Bachelor of Science degree in Computer Science from the United States Military Academy at West Point and a Master of Science in Computer Science from The George Washington University.

Over the past fifteen years, automation and the use of computer systems has permeated every aspect of modern life. Our Nation is entirely reliant upon computer systems and networked technologies in everything from national security and intelligence activities to commerce and business operations to power production and transmission to personal communications and correspondences.

Today's Internet has become one of the unifying fabrics driving globalization at an increasingly accelerated pace. Beyond its role as the pervasive communications medium, computer based automation and technology are the driving forces behind every major industrial and economic base in the world. Simply put, computer technologies and communications represent the greatest threat to and opportunity for our Nation.

Networking and Information Technology Research and Development (NITRD)

The United States leads the world in networking and information technology (NIT). In recent years competitors in China and India have been investing strategically in large scale NIT research and development efforts. The US leadership position is primarily driven by and can only be maintained by continuing with a broadly diffused and highly innovative industrial base in networking and information technologies. Simply put, we will lose if our efforts are reduced to long term direct and linear competition. The competitive landscape overseas includes large scale, well coordinated and deliberate investment into NIT research, development and education programs, which we cannot match. It is, in fact, our innovation which is necessary for continued leadership in technology. The NITRD program, which invests approximately $3.5 Billion, is a key component by which the US Government contributes to defining the federal need and contributing to national efforts in these areas.

Research or Development Balance and Focus

In order for NITRD to provide the maximum benefit to the Government and the Nation, it must work hand in glove with industry ingenuity and entrepreneurship. Every year through corporate programs and private industry, billions of dollars are invested in improving network and information technologies. According to the National Venture Capital Association, "Since 1970 venture capitalists have invested more than $466 Billion into more than 60,700 companies." Most of these investments are iterative improvements to technologies and methods which are known and are intended to develop and commercialize them, thereby making them broadly available. US Government networking and information technology needs align very closely with those of private industry. These areas of alignment are broad, including large scale processing, networking and storage platforms, human computer interaction, data and knowledge management, software and systems design, cyber security and information assurance (which include resiliency, integrity and confidentiality), and workforce issues. Only in isolated instances are Government needs unique or do they differ from those of industry. In cases where they differ slightly or in cases where the government-specific requirements represent a significant enough commercial opportunity, private industry will evolve to meet those unique needs as well. Technologies developed by private industry not only fuel economic growth, they provide for technologies better supported in the field, more nimble to evolve as requirements change and ultimately lower the total cost of ownership. However, only in rare instances does the private sector invest in fundamental or long term research activities, which must remain the focus of federal government R&D activities.

Classified Versus Unclassified Research and Development Activities

NITRD funds unclassified activities. Nearly all US Government funding for NIT research should occur at an unclassified level. In certain areas government-use cases of technology must remain legitimately classified, but the fundamental research behind these networking and information technology efforts must occur at the unclassified level. The vast majority of promising researchers do not hold adequate security clearances, which serves to significantly limit the talent pool for classified research. Fundamental research efforts when classified also prevent the nation from leveraging the innovation outside of the privileged few. This holds true for adoption by the private sector, NIT advantage and growth in private industry and consequently also a decrease in overall economic efficiency and competitiveness of the nation. Classified research programs lack the adequate public review and debate necessary to assure that the programs are designed optimally, contain the highest level of innovation, and are well-aligned with and informed by the total body of knowledge of the NIT community. In the rare cases where R&D projects must be classified, The White House Office of Science and Technology Policy (OSTP), which has the appropriate clearances, should work to ensure proper coordination and non-duplication with unclassified R&D efforts.

Cyber Security R&D

The current paradigm in cyber security is not likely to change significantly through private sector efforts in areas such as improved security products, monitoring and incident response capabilities. While the private sector makes significant investment in needed incremental product, application and protocol improvements; fundamental research is required to meaningfully improve the security of the cyber and critical infrastructures.

According to the CSIS Commission work, "The federal government plans to spend about $143 billion in 2009 on R&D. We estimate that two-tenths of 1 percent of that will go to cybersecurity." An inherently government investment must drive long term research agendas in cybersecurity, where private sector focus on shorter term commercialization limits gains to those of a more tactical and incremental nature.

NITRD programs will receive $3.5 billion for research and development, and cyber R&D will receive approximately $300 million. Beyond the $260 million reported by NITRD as being focused on cyber R&D, the Department of Homeland Security allocated an additional $19.5 million for 2009 in S&T programs for cyber that is not included in NITRD figures. Funding for research and development is politically complex and many of the groups who should be benefiting from it are not. A $300 million investment in cybersecurity is inadequate. DHS' embarrassing lack of attention to cyber programs simply fails any semblance of judgment and mocks their role as sector specific or lead agency on cyber matters. As cyber R&D portfolio manager at DHS, Doug Maughan has been very successful given an untenable lack of resources.

The Comprehensive National Cyber Initiative (CNCI) calls for increased near and longer term R&D activities. Care must be taken to not expend limited resources trying to enter the security product development business, especially via classified venues. Rather, the government must guide and assist in articulating functional requirements for the development of technologies that can help us best address the sophisticated cyber threat environment. These requirements must inform a broad reform of our sourcing methods for networking and information technologies so that they are procured, deployed and maintained in a more secured state. By appropriately relying on industry for development, we can avoid the problem of government development efforts stranding enterprise cyber defenders without the benefits of product management, maintenance or professional support. The resulting improvement in security technologies will not only benefit the government in protecting its systems, but will also benefit the nation's critical infrastructure operators and rest of the shared Internet fabric that joins our digital world.

A national research and development technology agenda must both identify the most promising ideas and describe the strategy that brings those ideas into fruition, recognizing that these activities must work hand in glove with private industry. The agenda must also jumpstart a multidisciplinary effort. By incorporating other disciplines that are greatly affected by cyber, we can better understand the security implications of their reliance on cyber and also help identify creative methods for addressing critical shortcomings.

The INFOSEC Research Council's "Hard Problems" list identifies several areas in need of immediate funding and action;

1. Global-Scale Identity – Identification required to produce an infrastructure capable of and reliable for commercial and national security purposes

2. Insider Threat – All security technologies and approaches rely practically on modeled behavior of external bad actors. This runs contrary to a majority of the security data, which shows damaged caused by insiders to be orders of magnitude more frequent and costly

3. Availability of Time-Critical Systems – Implementing effective security for systems where timeliness, performance and availability are higher priority services than security (i.e. control systems)

4. Scalable Secure Systems – The development of large-scale secure systems where individual components or dependencies may be flawed or compromised

5. Situational Understanding and Attack Attribution – Determining the current state of security for large scale and complex systems and being able to conduct assessments and provide attribution for security incidents

6. Information Provenance – Developing systems and methods to determine and manage the integrity of information and information systems

7. Security with Privacy – Designing methods and processes to improve security while preserving or enhancing privacy through granularity of activities and systems improvements

8. Enterprise-Level Security Metrics –Scalable methods to determine or represent security or risk are needed in order to optimize resource allocation and decision making.

Conclusions

In the areas of networking and information technologies Congress and the Obama Administration can meaningfully improve the impact of federal investment.

1. Focus on fundamental research that is currently unfunded, but necessary to assure America's long term competitiveness.

2. Except in rare instances, networking and information technology research and development should be conducted in an unclassified fashion.

3. While spending more on cyber security research and development activities in their aggregate is desirable, a redistribution of resources from government custom cyber security technology development to research activities would substantively increase the likelihood of discovering the paradigm changing methods which might take us out of the current cycle of tactical cat and mouse increments.

4. The Department of Homeland Security should invest meaningfully in cyber security research and development. The Intelligence Advanced Research Projects Activity (IARPA) should focus on top intelligence community problems, such as attack attribution, which may represent a hard problem, but does not represent significant overlap with the research needs of many other federal department and agency missions. Nor is attribution a research requirement of the private sector.

5. In a much needed redistribution of priorities from tactical government development efforts to the funding of fundamental research, a series of creative and lower cost programs can help the government better understand and leverage the emerging development efforts of private industry. As an innovative example of one such program, In-Q-Tel, a government funded, non-profit, venture capital entity actively reviews hundreds of innovative, venture capital-backed, emerging technologies each year from around the nation and selectively brings them to the Intelligence Community. These technologies can address near-term requirements or solutions the IC would otherwise likely fund costly development efforts to address. This innovative model not only assures efforts are informed by private industry, it also helps the government leverage capital already invested in the development of new technologies and spurs economic growth. Such innovative approaches can be used for greater alignment with industry.

Amit Yoran

Chairman and CEO, NetWitness Corporation
Amit@NetWitness.com, +1.703.889.8944

Amit Yoran serves as the Chairman and CEO of NetWitness Corporation, a leading provider of network security analytic products. He is a Commissioner of the CSIS Commission on Cyber Security advising the 44th Presidency and serves on several industry and national advisory bodies. Prior to NetWitness Mr Yoran served Director of the National Cyber Security Division at the Department of Homeland Security, and as CEO and advisor to In-Q-Tel, the venture capital arm of the CIA. Formerly he served as the Vice President of Worldwide Managed Security Services at the Symantec Corporation. Mr. Yoran was the co-founder of Riptech, a market leading IT security company, and served as it's CEO until the company was acquired by Symantec in 2002. He formerly served an officer in the United States Air Force in the Department of Defense's Computer Emergency Response Team

Mr Yoran is an independent director on the boards of innovative security technology companies Boards, including; Guardium, Digital Sandbox, and IronKey. He previously served on the board of Cyota until the company's acquisition by RSA in 2006, Guidance Software (GUID) through the company's successful IPO in 2007 and as an advisor to Intruvert Networks until the company's acquisition by McAfee in 2003.

Mr. Yoran received a Master of Science degree from the George Washington University and Bachelor of Science from the United States Military Academy at West Point.