Testimony of

Terry V. Benzel

University of Southern California, Information Sciences Institute

Before the House Science, Space and Technology Committee Subcommittees on Research and Technology

Hearing on
Cyber R&D Challenges and Solutions
February 26, 2013

Thank you Chairman Massie, Ranking Member Wilson, Chairman Bucshon, Ranking Member Lipinski, and Members of the Committee, for this opportunity to discuss Cyber Research and Development Challenges and Solutions. I am pleased to add my perspective on the Committee's questions, and my comments on the Cyber Security Enhancement Act of 2013. My remarks are based on more than 30 years in the cyber security research and development community, including:

- Senior positions at a Federally Funded Research and Development Center (FFRDC);
- Senior positions at a startup security company, Trusted Information Systems, that underwent a successful IPO and was acquired by a large enterprise security vendor;
- Vice President of Research at McAfee, Inc., then called Network Associates, and among the five largest software companies in the world;
- Special Projects Director at University of California at Berkeley;
- A consultant to cyber security start-up companies seeking Small Business Investigative Research (SBIR) grants;
- My present position with two roles: Project Investigator on a large DHS S&T - funded cyber security project; and Deputy Division Director at the University of Southern California's Information Sciences Institute, in the Cyber Networks and Cyber Security Division.

Given my experiences, I am passionate about the topics facing this hearing:

- Cyber-security threats to our critical infrastructure,
- The cyber component of homeland security,
- The R&D programs needed to create new cyber-defenses and stronger critical infrastructure,
- The coordination, collaboration and education that are needed for
    - technology transfer from R&D to practical cyber-defenses, and
    - building the next generation of cyber-defenders who will use the new technology created by R&D.

1. Background

First, let me provide some background on my current work. I am the Deputy Director of the Cyber Networks and Cyber Security Division of the Information Sciences Institute (ISI), part of the Viterbi School of Engineering at the University of Southern California (USC). USC is one of the world's leading private research universities and an anchor institution in Los Angeles, a city that is now a global center for technology, international trade and the arts.

The Viterbi School of Engineering has been a leader in the transformation from analog to digital communications since the early 1960s. In fact, ISI was one of the handful of institutions around the globe that created the Internet. Our researchers largely developed the Internet communications protocols that are still in use, administered the domain name system (DNS) for 16 years, and coined the terms "dot-com," "dot-org", "dot-gov" and "dot-net" that are now ubiquitous worldwide.

My comments on R&D, and on technology transfer and education in particular, are based on my whole professional history. They are informed by my work at ISI, which has unique whose unique characteristics are applicable to the issues facing this panel today. In particular:

- Our work spans three complementary and critical areas: **academic**, including research and education; **industrial**, delivering technology-based solutions for government and business partners; and **professional**, offering students unusual, hands-on experience.
    - All these components are required to pursue R&D that is well prepared for tech transfer and use by a well-educated technology workforce.

- Our research work spans *pure fundamental research* to *applied technology* that can be transitioned to practical use in government and industry. Numerous systems developed at ISI have been fielded in operational settings. Many have become the basis of new product offerings, either for startups or acquisition by established technology companies.

- Our reliance primarily on federal funding, our experience with applied projects and our role in educating the next generation of researchers, gives us an unusual, integrated perspective on research, education and technology transfer needs, processes and solutions.

In the cyber-security part of ISI, our work shares all these characteristics. My group's cyber-security work is focused mainly on the DETER Project, which is one of the nation's foremost resources for innovative, experiment-based cyber R&D. In DETER, we are working to address critical strategic issues:

- While cyber-threat growth continues to accelerate, the stream of new and effective cyber-defense technologies has grown much more slowly. The gap

between threat and defense has widened, even as our adversaries deploy increasingly sophisticated attack technology and engage in cyber-crime with unprecedented power, resources, and global reach. Moreover, targets increasingly are attacked with foreign state sponsorship.

- Our nation's cyber-adversaries are focusing not only high-profile commercial and government systems, and not only the traditional critical infrastructures such as the power grid, hydro dams, and nuclear energy facilities, but also new targets that affect individual health and safety: wireless computing and controls in cars, medical devices, home appliances and safety systems, and the emerging smart energy grid that is tying them all together.

Before moving ahead with my remarks and recommendations about the cyber security challenge and the Cyber Security Enhancement Act, I will comment on how my group's current work addresses this cyber-security challenge, including issues of, and promising approaches to, cyber-security enhancement.

The DETER Project

The DETER project is working to fill the cyber-security gap described above. We function both as a research project and as the operator of a major cyber experimentation lab, DeterLab. Our research agenda spans a wide range of innovative methods, technology, and infrastructure for the work of cyber-security researchers. We put our research results and innovations into practice in DeterLab, which enables researchers to experiment with and test their cyber-security advances. One strategic goal for DeterLab is to help researchers dramatically accelerate the pace of their work, shifting from repetitive, small-lab engineering to the repeatable, measurable scientific experimentation and testing that we enable DeterLab users to conduct.

DeterLab is a large-scale facility used by researchers from hundreds of institutions worldwide. We enable researchers to observe and interact with real malicious software, operating in realistic network environments, at scales found in the real world. Researchers use the knowledge they gain from their experiments to devise cyber-defense innovations and to build systems that are inherently more robust. My team continually is developing capabilities that support increases in experiment scale and that refine careful, repeatable controls on that research.

Let me repeat my point about rigorous, repeatable testing and a realistic, large-scale test environment. These capabilities address a historical problem in tech transfer: an innovation that works well in a predictable, controlled environment, but turns out to be much less effective, reliable or manageable in a major, critical government or enterprise IT environment. Without realistic, large-scale resources and research environments, results are unpredictable. As I observed when I worked for security vendors, large enterprise-security companies have been burned time and again by acquiring small security startups that are attempting to commercialize university-bred research. These

products may work well for a few early adopters, but rarely scale up to real enterprise environments in terms of effective protection or practical security management.

In DeterLab, we are continually extending the shared scientific facility to help researchers better prove their work in a realistic setting, and to better prepare for successful tech transfer. We – and our funders at DHS S&T and DoD – believe that realistic, scientific experimentation and testing is critical to advancing the scale, pace, and power of cyber-security R&D. As R&D accelerates, testing proves effective, and the cyber-research community grows, we are becoming better positioned to help bridge the growing cyber-security gap that endangers homeland security and critical infrastructure.

2. Cyber-Security Challenges Facing the Nation

Members of the House of Representatives, I would like to address four key points:

1. The importance of broadening the purview of cyber-security research
2. The importance of research infrastructure for experimental cyber-security research and development
3. The importance of new models for technology transfer from university research into commercial practices and products.
4. The importance of higher education for developing next-generation cyber-security researchers and technologies.

2.1 Broadening Cyber-Security Research

We face threats that are rapidly increasing in scope and sophistication. As was made painfully clear by last week's revelations of Chinese military incursions (by the "Shanghai Group" or "Comment Crew") into US systems, we now face state-sponsored cyber-sleuthing and cyber-terrorism. This unstable environment includes targeted attacks by ad hoc organizations and global cyber-crime syndicates that are escalating their operations against systems critical to our national safety and security.

Cyber security is now a constant challenge for every facet of civilized society. We have become completely dependent on cyber capabilities and, as a result, highly vulnerable to wide-ranging threats. Despite years of research, however, we are still at the losing end of an asymmetric battle. As members of these Sub-Committees, I'm sure you have heard many times that steps must be taken to change these dynamics. As a nation, we must support new forms of research and development, and must ensure that resulting advances are based solidly in experimental science.

But even the best work is meaningless unless a chain of activities works end to end.

- cyber- science must be transformed into meaningful technology;
- that technology must demonstrate its viability in real-world settings;
- real-world viability must become the basis for transferring technology to critical systems that otherwise remain vulnerable;

- critical systems operators must use and manage the new technology effectively;
- Efficacy must encompass the evolving landscape of threats.

If any one of these links falters, then cyber-security innovations will not deliver real value to government and commercial customers. Nor will they serve the ultimate stakeholders in those systems: you and I and our friends and family, all of whom depend on orderly air traffic, reliable electric power, secure personal data, an alert and ready military enterprise, and countless other vital services.

Too often, cyber-security research is narrowly focused on a few specific areas of investigation. Unfortunately, our adversaries also are doing theirR&D, and are planning their attack scenarios, without any of the same constraints. They are looking across multiple threat vectors for system vulnerabilities, within and across different technologies, and picking targets for their strategic value – not simply because they are easy marks.

For example, our community includes scientists conducting very good research on distributed denial of service threats, Internet worms, botnets and Internet routing attacks. Researchers typically specialize in just one of these well-known areas, where innovative countermeasures, protection and hardening are extremely valuable. But our adversaries are constructing attacks that combine these areas into even more potent, multi-faceted weapons. Often, these approaches are amplified with sophisticated social engineering attacks designed to steal the keys to vulnerable systems.

Fortunately, there is substantial progress away from the single-focus syndrome. Federal agency sponsors have been steering researchers toward cyber-security issues that are critical to national, homeland and economic security. One result is more breadth in cyber-security research. Another, perhaps more critical outcome is a shift away from existing, commercial cyber-security problems to those that are not yet subject to rigorous work. The National Science Foundation is pursuing this strategic approach through its Frontier, Large, Medium, and Center focused Secure and Trustworthy Computing Program (SaTC), and through other programs aimed at increasing research breadth and dimensionality. The DHS Science and Technology group funding also is helping shift research to difficult, nationally strategic issues.

Still, studying broadly within our own disciplines is not enough. Cyber-security is no longer solely an engineering discipline. It requires deep involvement from economists, sociologists, anthropologists and other scientists to create the holistic research agendas that can anticipate and guide effective cyber–defense strategies.

- **Recommendation #1:** ***Increase the breadth and scope of <u>strategic</u> cyber-security R&D, and create opportunities for multi-disciplinary research*****.**

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan, and specifically the call in item 2 for innovative, transformational technologies.

2.2. Research Infrastructure for Experimental Cyber Security Research and Development

Historically, cyber-security R&D has struggled to prove its value. The scientific basis for assessing the relative strength of theoretical and technological cyber-security solutions often has been uncertain. That uncertainty has hampered tech transition and widespread cyber-security adoption.

Corporations and government entities often pose security as a negative, as in: "We didn't get broken into, so we must be secure." In essence, t*hey define security as the absence of visible insecurity*. Even those that deploy cyber-security solutions may believe in simple, reactive "attack-defend-detect" approaches. Given my previous remarks and those of other cyber-security experts, it may seem puzzling that large-system organizations retain such a naïve position. I'd like to explain from personal experience how this mindset came about, and how a different approach to R&D is shifting the paradigm.

When I was a Vice President at McAfee, I often met with top corporate customers, which typically were large enterprises in banking, manufacturing, retail and other industries. The chief information officers of these organizations typically would ask me about return-on-investment (ROI) for our products. Their concern was how much to spend on, and how to best leverage, their cyber security investments. The truth is that we had no easy answers. At any single point in time, these customers could assess their threats and risks, and make rational choices on what defenses to purchase and why. But the threat environment changes so rapidly that *those choices might be sensible only at that specific moment, based on what was limited knowledge we, and the customers, had at the time.* Later, some choices might prove to deliver little value, while others were far more than worth their price. Still other, more devastating threats might remain threateningly at large.

This is a serious issue. Companies, particularly those with public shareholders, can't sit still and ignore the latest security technologies lest they find their systems seriously compromised. Security vendors have every incentive to reinforce that knowledge. They continuously can deliver new security widgets to counteract newly discovered threats. Some of these "solutions" invariably will be ineffectual or impractical. Are customers' threats addressed and risks reduced overall, at any increased rate? While there was and is no way to measure, the answer appears to be a resounding "No." We now see the world's most extensive, sophisticated IT operations, in corporations and governments worldwide, penetrated by China, Iran, organized crime and other top-tier adversaries.

Given the fundamental flaw in reactive approaches, a community began to emerge in around the year 2000 to create a *science* of experimental cyber–security. We saw a need to build environments that would:

- support experimentation and testing of hypotheses;
- enable creation of repeatable, science-based experiments that could be validated by others;
- generate research results that could be leveraged into broad, multi-component solutions in which components demonstrably support one another, making the whole greater than the sum of its parts.
- foster methodologies and tools to help guide experimenters toward this new, scientific cyber-security, and provide an open environment for researchers in industry, government and academia to build on one another's achievements.

Under funding from Dr. Douglas Maughan, then at DARPA, we performed a study, "Justification and Requirements for a National DDoS Defense Technology Evaluation Facility." The study provided the basis for defining key objectives for the DETER project. In 2003, with funding from NSF and DHS S&T, we initiated the DETER Project.

Looking forward, it is clear that cyber security R&D must be grounded in the same systematic approach to discovery and validation that is routine in other scientific and technological disciplines. To approach these challenging research problems, *we must create a paradigm shift in experimental cyber-security*. Only by enabling demonstrable, repeatable experimental results can we provide a sound basis for researchers to leverage prior work – and create new capabilities not yet imaginable. Tomorrow's researchers must be able to stand on the shoulders of today's researchers, not be consigned to re-treading the same ground.

Only by living in the future – enabling researchers to experiment with techniques and tools that do not yet exist and operate in environments only beginning to emerge – can highly capable, fluid new approaches take shape. The alternative is to remain caught on the new-widget treadmill, in which the nation must continually run faster to stay in same place, while invariably falling behind.

Living in the future also means enabling continuous R&D infrastructure gains. Our highly connected world is growing exponentially in scale and complexity. Critical national assets, and the threats to them, evolve in tandem as well. While there are now various cyber-security testbed experimentation facilities around the U.S., only a few are applicable to a wide range of experimentation and almost none are openly available. Still, their existence is a valuable step toward research into a cross-disciplinary range of cyber-security experimentation and testing methods and tools.

NSF, DHS S&T, DOE and DARPA all have invested in this evolution, spurring valuable advances such as federation of diverse scientific facilities. Researchers in disparate

locations now are able to work collaboratively, at the same time, to conduct experiments on a global scale.

But these advances are circumscribed and uneven. To match dramatic, ongoing change and complexity in the world at large, our cyber-defenders need parallel growth in R&D infrastructure capabilities. These initiatives must be expanded and coordinated to support a highly capable, shared national resource.

- **Recommendation #2:** ***Formulate a research strategy/agenda to develop open, broad, multi-organizational cyber-security experimentation and testing capabilities.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan. Specifically, item 4 requires a plan to "maintain a national research infrastructure for creating, testing, and evaluating the next generation of secure networking and information technology systems."

2.3 Technology Transfer

The U.S. government and major corporations have poured hundreds of millions of dollars into security R&D for more than 20 years. Creditably, this spending is growing in scale and increasingly is strategically focused on critical infrastructure and homeland security. These investments hold the promise of delivering real-world value: putting practical security technologies in place to protect important assets. Of course, I recommend that funding agencies continue to grow their emphases in these crucial directions.

At the same time, however, troubling technology-transfer issues remain. As Members of this committee and its sub-committees, you may wonder: Why is technology transfer so difficult? Why does so much promising research not find its way into viable commercial products? Why do specific needs of specific government agencies and departments remain unaddressed?

In part, the answer lies in what I've already discussed: that security R&D has tended to be ad hoc, small-scale and lacking in the scientific methods of other disciplines – and thus in creation of a solid, accessible body of knowledge. But there also have been, and continue to be, structural problems with current tech transfer processes that can't be solved through hardening the science alone. Researchers and funders could achieve our wildest dreams for effective, cost-efficient, privacy-assuring cyber-security. Yet the results might have no impact unless the underlying structural issues are addressed and resolved.

These issues historically have included:

- *Insufficient awareness of the complexity of cyber-security tech transfer.* Tech transfer, while difficult in any field, seems particularly so in the constantly shifting world of cyber-security. At each stage from initial research idea, advanced prototype and early stage product to widespread adoption, the process can break due to internal factors or sudden shifts in attack methodologies, tools and strategies. Commercializing security technologies effectively accordingly has been, in some cases, largely a matter of chance.

- *A scatter-shot approach to R&D.* Over the last 40 years, governments and businesses around the globe have invested hundreds of millions of dollars in cyber-security R&D – but only loosely in coordination with one another. Research often was initiated based on a largely reactionary model driven by the hot security topic of the day.

- *Mismatch between market and threat environment*. Security vendors became very tactical in focus, looking at which innovations would fuel the next incremental security fix. They then upsold to existing customers and attempted to pull in new ones.

- *Assumptions of contained damage*. When a major cyber-attack occurred in the 1990s, businesses and governments were forced to reboot a few thousand systems. The scale and pervasiveness of computing technology has grown so dramatically that such an approach is now wholly unfeasible.

As a result of this largely ad hoc approach, some government and private investment has sparked revolutionary new products, companies and industries. Others have improved the operational security practices of IT departments around the world dramatically. Still others have resulted in research papers and prototypes, but not commercializable technologies. The net effect is that many potentially valuable security technologies never saw the light of day.

Fortunately, the situation is improving. Tech-transfer issues are being mitigated as researchers and funders set more realistic expectations and achievable goals. Businesses better understand that stellar approaches must be combined with sharp execution in operations, finance, sales and marketing. An enormous, interconnected world market also has forced research institutions and businesses to make more strategic choices in the technologies and approaches they pursue.

New approaches to tech transfer also are paying – often literally – dividends. For example, the Stevens Institute for Innovation at USC, funded by highly successful venture capitalist Mark Stevens and his wife, assists faculty and students with everything from nuts-and-bolts contracts and funding issues to instilling a culture of innovation university-wide. Its reliance on public-private partnerships, while not unique to USC, offers a uniquely effective means for engineers, physicians and other academic researchers to connect with the world at large.

In recent years, cyber-security R&D has been steered toward a model directed at homeland security and critical infrastructure. This strategic shift is fostering collaborations between universities and national labs, and is beginning to yield excellent work on smart energy grids, advanced persistent threats, next-generation Internet, and other security innovations that meet specified, high-priority needs. Much of this work is both strategic and long-term in nature, with the potential for fundamental transformation in protected assets or their protections.

Unfortunately, general enterprise security vendors have gone in the opposite direction. Most are now completely tactical, rather than strategic, in focus. As long as the cyber-security market was expanding dramatically, businesses could afford to pursue numerous, promising approaches. But market growth for these large-enterprise vendors largely has stalled despite the proliferation of technology. Large security vendors, like all players in mature markets, are chasing incremental growth in revenue and market share. They are dependent on creating small-scale innovations that will fuel the next incremental security fix. The vendor with the longest list of Band-Aids has the competitive edge.

At the same time, the majority of critical infrastructures are privately owned and operated in highly regulated industries, leaving them cost-constrained and lacking in capital for new technology. These industries also constitute narrow vertical markets that do not drive commercial product cycles. Such an approach is completely at odds with securing critical cyber infrastructure – and with strategic, long-term, transformational innovation.

In my view, it's imperative that we invent a new virtuous cycle in which government-funded work steers strategic cyber-security R&D. Clearly, the nation would be foolish to rely solely on incumbent vendors and system integrators to decide which innovations should be pushed forward and which consigned solely to professional journals. Public private partnerships and other innovative approaches surely can help re-define what the market is and how its vital players should be approached, For instance, the overall market may include not just large enterprise systems, but control systems for transportation, dedicated distribution like pipelines, and other businesses that deal in critical infrastructure. I don't know what this tech-transfer model ultimately will look like, but the current model flings open the door wide to cyber-***in***security.

There is, however, another structural issue: the businesses and government entities that are major security customers. Beginning in the 1990s, hydroelectric power plants, chemical manufacturers on major waterways, nuclear plants and other entities crucial to public safety began running control systems to monitor and manage their operations. Such systems theoretically separate their critical national assets from other systems connected to the Internet – and thus vulnerable to outside attack. Many control systems have known vulnerabilities, however, that are only partially addressed by commercial security products. While innovative security technologies exist to harden these systems, customers are slow to adopt them.

The reason: For decades, the security vendors on which these customers rely have offered assurances that current technology is "good enough." To admit otherwise might

require major, costly infrastructure changes for their customers. In highly regulated markets with limited capital, vendors are better served by continuing offer "good enough" and incremental low-cost Band-Aids.

As a result, the new virtuous cycle also must build sharply heightened threat awareness into customers' mindsets. Businesses and government entities must understand the magnitude of threats, the dire risks of miscalculation – to health and safety, citizen and consumer trust, and public and private finances – and that the disruption of the technology status quo may be more than worth the benefits. Customers must demand the level and pace of transformative technology that Americans deserve. Again, I don't presume to know how this should be done, only that it is as vital a mandate as advancing cyber-security defenses themselves.

In sum, the research challenges I described initially are compounded by significant tech transfer challenges. These challenges are surmountable if we:

- Continue steering security R&D firmly toward national strategic goals.
- Use public-private partnerships and other approaches to define or redefine markets and opportunities not served by incumbent security vendors.
- Find ways to engage customers in their own protection, both for the benefit of organizations and of the Americans they serve.

- **Recommendation #3:** ***Develop new models of technology transfer operation, funding, partnership and cultural change within organizations.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 103, Cybersecurity Strategic Research and Development plan. Specifically, item 3 calls for programs that, "… foster the rapid transfer of research and development results into new cybersecurity technologies and applications for the timely benefit of society and the national interest…"

2.4 Educating the Next Generation of Cyber-Security Researchers and Professionals

Beginning to change the asymmetric dynamics of cyber-space requires astute, knowledgeable researchers, educators, operators, users and citizens. But we as a nation are nowhere near that goal. Rapid growth and spread of information technology, dramatically increased system complexity, and the multi-dimensional interdependence of these systems have left us woefully unprepared on many fronts.

The current dearth of cyber-professionals has sparked significant new federal training and education programs aimed at addressing this need. Among these initiatives: the National Initiative for Cyber Security Education (NICE), the Scholarship for Service program, the National Centers of Academic Excellence in Information Assurance Education, and the Centers of Academic Excellence in Research.

While these initiatives are beginning to increase the pipeline of cyber-professionals, their scale, pace and depth so far are nowhere near sufficient to address America's critical

needs in the public or private sectors. The challenge now is to help government agencies, contractors and critical infrastructure providers locate and access program suited for their organizations' needs.

Just last week (on February 21, 2013), the U.S. Department of Homeland Security (DHS) launched the National Initiative for Cybersecurity Careers and Studies (NICCS), an online resource for cyber-security career, education, and training information. NICCS will help expand, inform, monitor, certify and promote training programs. The process of creating, cataloging and monitoring training programs is a positive step toward meeting the nation's pressing cyber-security needs.

To fundamentally change the cyber-threat dynamic, however, we need deep intellectual resources as well. These are represented by the brightest, best trained, most curious and most ambitious researchers and educators. We accordingly need to be prepared to make significant investments in higher education. I applaud the efforts of the NSF and other federal research agencies to create and fund cyber-security research and education grants. These fundamental research endeavors are the essential catalyst for research breakthroughs. Only by educating the next generation of researchers and educators today can we build the intellectual resources vital to solving tomorrow's problems.

USC actively is engaged in several new initiatives to advance cyber-education. The USC Viterbi School of Engineering offers classes in computer security, and recruits and funds graduate students who are exposed to leading-edge cyber security research. In addition, the University will begin offering a Master of Cyber Security degree. This novel degree, which will integrate strong engineering and computing theory with applied science, will educate students to help solve real-world information security challenges.

While classroom study and early exposure to research provide foundational cyber-security education, effective training also demands direct, hands-on involvement. Teaching cyber security is challenging. How do you demonstrate system weaknesses, inspire students to create constructive new solutions to vulnerabilities, and provide an environment in which they realistically can explore threat scenarios? We believe that undergraduates with direct cyber-security experience are most likely to be eager to – and capable of – earning master's degrees. Similarly, graduate students who engage in science-based experimental research are most likely to develop the passion to pursue demanding doctoral and post-doctoral studies, and to obtain the academic positions that will enable them to continue developing our nation's cyber-warriors. None of these advances would be possible without federal government investment in fundamental cyber-security research.

The DETER Project at ISI offers precisely the hands-on security education, to a wide range of colleges and universities, that is essential for strengthening our intellectual resources. Teaching cyber-security is a core component of DETER's two-fold mission: to develop research into capable new cyber-security methods and technologies, and to operate DeterLab, our shared facility for cyber-security experimentation, testing and education. Through the DETER Project, educators can tap into DeterLab, providing

students with the vivid, realistic experience that can spark imagination and ignite passion for research.

DeterLab also fills a significant gap in security instruction by providing educators worldwide with substantive, thoroughly vetted facilities and materials. These security lab exercises complement existing, more abstract courses, enabling students to see and feel the phenomena they learn in classrooms. Instructors and students conduct lab exercises using DeterLab's dedicated hardware, networks and customized Web-based interface.

We need to develop a new generation of cyber-security researchers who are brought up in the world of R&D performed in realistic settings, and we need to provide the resources necessary for realistic, scientific testing and experimentation. We need to develop the research community to be part of the invention of new models of R&D and tech transfer. We cannot hope to begin to change the dynamics of the asymmetric cyber space if we don't have knowledgeable researchers, educators, I.T. operators, users and citizens.

- **Recommendation #4 –** ***Increase educational programs in cyber-security research and development, with an emphasis on doctoral degrees.***

The Cybersecurity Enhancement Act of 2013 includes provisions for addressing this recommendation in sec. 106, Federal Cyber Scholarship For Service
18 Program; sec. 107, Cybersecurity Workforce Assessment; and sec. 108, Cybersecurity University-Industry Task Force.

3. Summary

Cyber security is now a constant, serious and accelerating challenge in every facet of American society. We have become completely dependent on cyber capabilities and, as a result, highly vulnerable to wide-ranging threats. Where these once were largely annoying hacker probes and network intrusions, we now face organized crime and state-sponsored cyber-terrorism. Despite many years of research, we are still on the losing side of an asymmetric battle. These dynamics must be changed to protect US government information, corporate trade secrets, and public health and safety, among other vital concerns. We can no longer treat cyber security as an engineering discipline, we must embrace multiple disciplines bringing economists, sociologists, anthropologists and the other sciences to the table to create holistic research agendas.

Increase the breadth and scope of cyber-security R&D, and create opportunities for multi-disciplinary research.

Corporations and government entities often define security as the absence of visible insecurity. Cyber-security R&D often has been small-scale and ad hoc, and has struggled to prove its worth. Research must be grounded in the same systematic approach to discovery and validation that is routine in other scientific and technological disciplines.

New approaches to research and development must be energized – and new findings must be based in hard experimental science – to support crucial cyber-security discovery, validation and ongoing analysis. Only by enabling demonstrable, repeatable experimental results can we provide a sound basis for researchers to leverage prior work – and create new capabilities not yet imaginable.

Formulate a research strategy/agenda to develop open, broad, multi-organizational cyber-security experimentation and testing capabilities.

Technology transfer is particularly difficult in the constantly shifting world of cyber-security. At each stage from initial research idea, advanced prototype, early stage product and widespread adoption, the process can break due to internal factors or sudden shifts in attack methodologies, tools and strategies. The net effect is that many potentially valuable security technologies never see the light of day. Commercializing security technologies in some cases has been largely a matter of chance.

Develop new models of technology transfer operation, funding, partnership and cultural change within organizations.

The U.S. needs deep intellectual resources to change the cyber-threat dynamic fundamentally. In addition to creating, cataloging and monitoring training programs, we need to be prepared to make significant investments in higher education. I applaud the efforts of the National Science Foundation and other federal research agencies to create and fund cyber-security research and education grants. These fundamental research endeavors are the essential catalyst for research breakthroughs. Only by educating the next generation of researchers and educators today can we build the intellectual resources vital to solving tomorrow's problems.

Increase educational programs in cyber-security research and development, with an emphasis on doctoral degrees.

Taken together, these four recommendations form the basis for a multi-pronged, sustainable national program to address cyber R&D challenges – and to pursue the most promising approaches to a new order for research, development and innovation partnerships.