Testimony before the House Armed Services Committee
Hearing on
"Cyber Security, Information Assurance and Information Superiority"

27 October 2005

Statement of
Eugene H. Spafford

Professor and Executive Director
Purdue University Center For Education and Research in Information Assurance and Security (CERIAS)

Chair of The U.S. Public Policy Committee
of The Association For Computing Machinery (USACM)

Member of the Board of Directors
of the Computing Research Association (CRA)

Table of Contents

Introduction 1

Summary of Threats 2

Specific Threats 3

Exacerbating Conditions 4

Some Recommendations 7

Questions from the Committee 9

Conclusion 11

Acknowledgments 11

Introduction

Thank you Chairman Hunter and Ranking Member Skelton for the opportunity to testify at this hearing. Threats to information systems have been steadily growing in number and sophistication over the last two decades. They currently present a substantial danger to the U.S. military, the civilian government, industry, academia, and the general public. So many of these systems are interconnected and dependent on each other that threats to one segment often spread to all the others. Because many of these threats use victim computers to perpetuate the attack, it presents an asymmetric threat to which U.S. computer systems are particularly vulnerable. In the remainder of this document I will briefly outline a few selected aspects of the problems involved that are especially important; a full treatment of all the issues would represent a major volume. The complex interplay of the various components of our IT infrastructure mean that there are no simple fixes for the problems we face. The best solution is to continually enhance and sustain our capabilities to address cyber security problems, exactly as we do for other significant threats.

I will limit my comments to issues related to Computer and Network Defense (CND) issues, as the specific questions posed to me were primarily about defense. Issues of CNA (attack) and CNE (exploitation) are also involved in the overall context of Computer and Network Operations (CNO). Details of CNA and CNE capabilities are generally highly classified, and I therefore am unable to comment on them. However, given that potential foreign targets are using many of the same products as those used by our own DoD, it would seem that other countries are currently as vulnerable to cyber attacks as our military.

By way of self-introduction, I am a professor at Purdue University with a joint appointment in the department of Computer Sciences and the school of Electrical and Computer Engineering. I also have courtesy appointments in the departments of Philosophy, Communication, and the College of Technology. I am also the Executive Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we have a set of affiliate university programs working with us in a number of states, including Illinois, Iowa, North Carolina, the District of Columbia, Ohio, Virginia, Idaho, and New York. CERIAS also has a close working relationship with a dozen major commercial firms and government laboratories.

In addition to my role as an academic faculty member, I also serve on several boards of technical advisors, including those of SignaCert, Unisys, Microsoft, DigitalDoors, and Open Channel Software; and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I was a member of the most recent incarnation of the President's Information Technology Advisory Committee (PITAC) from 2003 to earlier this year. I have been working in information security for 25 years.

I began this document by listing my affiliations with ACM and CRA. This testimony is not an official statement by either organization, but is consistent with their overall goals and aims. ACM is a nonprofit educational and scientific computing society of about 80,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. The Computing Research Association is an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is particularly interested in issues that affect the conduct of computing research in the USA.

Summary of Threats

I will not attempt to summarize the magnitude of cyber threats currently facing our information infrastructure, including our Department of Defense. There are many reports describing these threats, including reports from the PITAC, the GAO, the National Academies, the Department of Justice, and many commercial entities. From these reports the following general trends may be derived:

- The number of reported attacks of various kinds is generally increasing annually;
- Attacks are becoming more sophisticated and more efficient;
- Few perpetrators are ever caught and prosecuted;
- An unknown (but probably large) number of attacks, frauds and violations are not detected with current defenses;
- A large number of detected attacks are not reported to appropriate authorities;
- The problem is international in scope, both in origin of attacks and in location of victims;
- The majority of the attacks are enabled by faulty software, poor configuration, and operator error.

The Department of Defense operates many computers and networks that are little different from those of other government agencies and private organizations. They are prone to some of the same faults, misconfigurations, and operator mistakes. However, the DoD is an especially sensitive target because of its role in securing the national defense and projecting US policy. As such, it is subject to probing and attack by actors, such as national intelligence services, who might not be interested in most commercial systems. However, vandals and anarchists will be as interested in attacking DoD systems as they would in attacking other government systems. Criminal elements may well be interested in attacking Defense systems to obtain sensitive information for sale or use, to steal supplies (including weapons), to obtain intelligence that may impact their operations (e.g., military involvement in drug smuggling interdiction), and to gather information for fraud (e.g., identity theft).

To date, DoD systems have continued to fall prey to various forms of attack by these actors, and by actors unknown. Computer viruses and worms have spread throughout Defense systems, including some classified systems. Intruders have gained access to sensitive systems and data. Information has been taken from DoD systems and used for purposes of fraud as well as common espionage. Systems have been taken down and contaminated by unknown parties of foreign origin. Network floods have disabled access to DoD systems. Undoubtedly the magnitude of the problem is greater than has been openly reported, and more has occurred than has been detected. I have every confidence that such incidents will continue to occur.

If this variety and magnitude of incidents were to occur to physical resources – unauthorized access to sensitive data, disclosure of personnel information, significant fraud, espionage, and degradation of function – there would be widespread outcry, investigation, and significant disciplinary action against those in charge. Unfortunately, we have developed an attitude and culture that views failures and compromises of important computing systems as inevitable and acceptable. This is dangerous, and threatens the future economic and military safety of the country.

Specific Threats

There are many threats to our IT systems, and to DoD systems in particular. As the DoD employs large amounts of COTS (commercial off-the-shelf) products, or uses partially modified COTS products in GOTS (government off-the-shelf) products, they are prey to some of the same vulnerabilities as we see in the private sector and elsewhere in government. The threats are largely the same, although the specific targets and consequences may well be different.

Not only are Defense systems based on common COTS products and protocols, but they are often interconnected with (and dependent on) the private sector. The vast majority of DoD network communications flows over private telecommunications networks, for instance. Military logistics systems are often directly connected to civilian suppliers so as to provide direct B-to-B (business-to-business) ordering to enhance speed and reduce cost. Military analysts are connected to online news and search sites for open-source intelligence. Email is interconnected. Other connections and dependencies also exist: some known, and many largely unknown. It is important to realize that the DoD, despite some efforts to the contrary, is intimately connected to the rest of the national (and thus, international) IT infrastructure. Even plans for the future Global Information Grid (GIG) will not serve to disconnect these systems completely.

There are thus many pathways for attacks to occur against DoD systems (as well as other government systems), and such connectivity will continue to exist (and is actually necessary for many reasons). In the following, I will outline, generally, where I have observed potential weaknesses in DoD IT systems:

> Malicious software such as viruses and worms. Software that is self-propagating uses the connectivity and power of victim computers against themselves and others. The homogeneity of DoD systems makes them especially vulnerable to well-crafted malicious software.[1] A carefully crafted computer worm could cause disruption of operation, denial of service, and corruption of information on large numbers of DoD systems.
>
> Insider threats. I have observed deficiencies in internal protection and counterintelligence operations at many DoD and government facilities over the last decade. At the same time, the military has experienced an increase in the use of civilian consultants and contractors, increased collaboration and exchange with foreign partners, and an increase in US citizens involved in acts of terrorism based on idealism. All of these increase our risk of insider attacks against key systems and data. Without adequate internal safeguards against insider threats – both technical and operational – we are needlessly exposing our systems and data to damage and exploitation.
>
> Infiltration. Our military and government rely on COTS products and contractors to equip and staff our IT infrastructure. Consider that some of those products that are employed in highly sensitive applications are being crafted, tested, packaged and supported by individuals who would never be allowed into the locations where those applications are used because of national origin, criminal history, and/or personal behavior. Furthermore, some of the hardware and software components in use in critical applications are designed and produced in countries that may be adversaries in future military or political conflict. These factors enable "life cycle" attacks where key systems can be compromised during early manufacture, shipping, and maintenance as well as end operation. We do not have the tools or resources to thoroughly check these items to ensure that they do not have "hidden features" or flaws that may be used against us. We need special attention and methods to produce these supervisory systems and critical applications.
>
> Denial of Service. We currently depend on our networks and computing infrastructure. Effective denial of service attacks against key systems would be devastating. These attacks could be totally IT-based, as in network flooding against DoD communications sites, to large

[1] I provided extensive written testimony on the threat of malicious software to DoD computers to a subcommittee of this committee on 24 July 2003.

scale physical attacks such as EMP (electromagnetic pulse) weapons used against whole theaters. Some systems in some sites are protected against such attacks, and there are some alternative systems and networks in place. However, I question whether sufficient planning and risk assessment have been uniformly performed on scenarios where significant loss of capability might occur. Without capable alternatives, our military would be significantly handicapped.

Data Contamination. Many of our DoD systems depend on large data stores. These include textual data such as personnel records, geospatial data such as maps and targeting coordinates, and image data including parts diagrams and surveillance photos. Too few of these records are protected against subtle alteration by outsiders. This protection might occur through the use of immutable storage media, internal consistency checks, and digital signatures. Gross changes, such as deletion, could be quickly spotted and repaired through the use of backups. There is a danger, however, of long-term, subtle changes that alter key data without the changes being detected. For instance, alteration of a few targeting data for a theater of operations might result in multiple civilian targets being attacked in error, leading to political damage and loss of confidence in the military systems in use.

All of these threat classes are real, and examples of all but the last can be readily found in the open literature. I have seen little reasonable planning to address these threats, either within the DoD or within the US government in general. Instead, the approach that is in widespread use is to employ greater control over patching of some known flaws, and increasing the strength of some perimeter defenses. Neither of these approaches addresses the underlying problems, and neither appropriately anticipates future threats.

It is difficult to anticipate new threats that will emerge. Many experts believe the increasing adoption of new technologies without careful consideration of risks will open new avenues of attack. Two examples are the increasing use of wireless networks and voice-over-IP (VoIP) telephony. Each of these offers new opportunities for convenience, mobility, and cost savings. However, both technologies are more easily disrupted and intercepted than the traditional technologies they replace. Other technologies being considered for future use include sensor networks, telepresence, and grid computing. Without careful consideration of risks and defenses, these may provide new opportunities for enemies and criminals to attack our IT infrastructure.

Equally of note is the increasing sophistication of the average attacker. As more value becomes accessible via computer networks, there is a greater criminal element involved in cyber activities. We should not underestimate that criminal element, especially as it includes individuals from countries around the world. Not only will they increasingly target government resources for their own gain, but some of them will undoubtedly operate on a "for hire" basis. Operating from countries with weak law enforcement and hostility to the United States, these individuals pose an unconventional threat that the military is not well equipped to handle.

Exacerbating Conditions

There are many factors that further enhance the vulnerability of DoD (and other) IT systems, and that will continue to endanger us in the future. I believe these six are among the most significant.

Over-dependence on COTS products. Several decades ago, the US Department of Defense was the world leader in the development of innovative software engineering methodologies for producing safe, effective computing products. However, almost all of the funding and in-house research in these areas was abandoned because of concerns over cost, and the delay of getting products fielded that met quality standards. There was also the belief that commercial systems with more features were better than limited, special-purpose military systems. The underlying assumption was that the marketplace would drive commercial firms into developing better methods and better software.

Unfortunately, the market responded differently than anticipated. The vast majority of customers continue to want fancy new features rather than high-quality, robust software. Given the choice, the majority of consumers will not pay extra for enhanced security, nor will they easily tolerate some of the limitations that such security would impose. The market has moved to continue to satisfy those desires and biases. Thus, the military is presented little choice but to acquire COTS products to satisfy IT needs, it is also forced to use products that contain large numbers of flaws, and that are designed for a very different threat environment than where they are used: most vendors design for supporting computer game playing at home and not joint force command and control in a real battle! Furthermore, government acquisition is usually influenced more by cost than by fitness for purpose. If branches of the uniformed military services were to acquire weapons platforms in the same manner, the Army would be strapping howitzers to pickup trucks, the Air Force would be dropping JDAMs from two-seater propeller planes, and the Navy would be patrolling the oceans in converted fishing boats.

Furthermore the market effectively demands that vendors regularly introduce new features to sell new product every few months or years. The new features add complexity, which adds new flaws, and in turn, adds new methods of attack. The additional complexity also means that the operators and maintainers of the systems have an ever more complex environment to understand and protect.

Many of the IT systems in use in the DoD today are vastly more complex and feature-laden than needed. The typical desktop computer has far more functionality than is needed for most applications, and thus more vulnerability than is prudent. However, because the DoD depends on market solutions and lowest cost bids, there is a vicious cycle which results in continued dependence on the same COTS products that have caused so many problems to date.

What is needed are policies and tools that enable us to extract the most valuable aspects of commercial systems, especially in low risk environments, so as to take advantage of commercial innovation and economy of scale. At the same time, we need to understand when and where to restrict the use of such systems so as not to increase our exposure to attacks.

No metrics. We have no good metrics to measure safety, security, and quality of IT products in a general and meaningful way. Therefore, we have no good method of comparing systems against each other, or of determining whether a system's overall security posture is improved by a configuration change. A simple count of the number of patches issued or applied is not sufficient, as this usually only reflects the responsiveness of the vendor. Neither does a count of the number of attacks detected and repulsed represent strength of defense, as this simply reflects the *detected* attacks *so far*. We need metrics that measure the resistance to attack of individual components, but more critically, we need metrics that can be used to evaluate whole systems of components as it is systems that are attacked.

What few metrics we do have, such as the Common Criteria, are intended to be applied against severely constrained configurations that are seldom actually deployed. Once options are changed and configurations modified, the original evaluations are no longer appropriate, and often mislead the uninformed about the security of their systems.

Lack of deterrence. Nationally and internationally we have almost no deterrence. Vandals and criminals can and do attack our IT systems with impunity because they know there is almost no chance of being caught unless they are exceedingly careless. We have primitive forensic capabilities and insufficient resources devoted to investigation and prosecution. We also have questions of jurisdiction domestically and internationally.

As a result of the lack of deterrence, acts of vandalism and cyber crime are on the rise. Not only is this damaging in and of itself, it provides a screen for more malicious activities: intrusion detection and analysis software is so overwhelmed with "chaff" that it may be unable to pick out the slow, deliberate, and skillful acts of espionage and sabotage that may be occurring.

Lack of fallback alternatives. I have observed great reliance within the DoD and government in general on IT. Too often there is no planning for how to proceed with critical mission responsibilities with degraded or disabled IT resources. This may be a failure to adequately envision and quantify risks, or where cost has driven decisions that amplify risk.

Under-investment in research. The current attitude within government as a whole, and in DoD in particular, is that long-term research is an option that can be cut given other budget needs. Simultaneously, the real and pressing needs of current patches and defenses get a huge share of resources. As was stated in the PITAC report, *Cyber Security: A Crisis of Prioritization* (and elsewhere), this shortening of the horizon means that we will be at a disadvantage in years to come. Innovation cannot be scheduled, nor can it be "caught up" with short deadlines and short-term increases in support. The research base needs to be supported consistently, over time, to build a body of results and a community of scholars. Cyber security (and many other areas of IT) does not have that community of scholars, nor do those researchers have the funding necessary to innovate as needed. Insufficient funding leads researchers to be more conservative, and less likely to address big problems. In the long term, this means we will continue to expend massive resources on fixing badly-broken, inappropriate systems rather than deploying more resilient, better defended systems.

There is an analogy here to what we have seen with Hurricane Katrina: it was known for some time that an unusual event could be catastrophic, and that contingency measures needed to be developed. However, full funding was not allocated as other needs appeared to be more pressing. Unfortunately, when the crisis came, there was no way that the needed responses could be put into place quickly enough to avert the full scope of the disaster. Similarly, the more we put off investing in finding solutions to the cyber security problem in favor of short term needs, the greater the damage will be when the disasters occur.

Consider that other countries are increasing their support for long-term IT research. This may lead to a future where important patents and key capabilities are held in countries other than the USA, and where we are forced to obtain critical resources for our defense from potential adversaries because we do not have the expertise nor infrastructure domestically to meet the need.

The PITAC report, and reports cited in it all speak to this issue. The PITAC found, in particular, that a shortening of the horizon in research funded by DARPA and by other DoD agencies coupled with changes in emphasis have had a negative effect on the field. This is only expected to get more pronounced in the coming years unless definitive action is taken to reverse the trend.

For example, figures compiled by the CRA show that DARPA funding for university-led research has declined by $100 million since 2001 despite a nearly $1 billion increase in DARPA's budget over the same period. More relevantly to the subject of this hearing, DARPA support for university-led computer science research has plummeted, from $198 million in FY 01 (adjusted) to $108 million in FY 04 (adjusted).

We should not depend on the marketplace to address this issue. US companies are driven largely by near-term profits and results. As a result we have seen a decrease in long-term intramural research by US industry, and a decrease in extramural funding of long-term research. Additionally, as I mentioned above, non-US companies may become very significant players in the marketplace, and we should be cautious about depending on their solutions.

These trends do not bode well for US defense.

Ill-informed application of classification. Over the last few years, there has been an increasing trend by various governmental agencies to classify anything to do with cyber security defense research, and to limit the participation of non-nationals in related research. This is usually misguided and definitely counterproductive.

There is no question that research into technologies for cyber offense should be closely guarded. However, given the extensive use of COTS products and commercial infrastructure, the only way we will enhance DoD cyber defenses is if improvements are made in publicly-available systems. It is not possible to do this while classifying the research and results! This issue was also investigated and discussed at length in the PITAC report.

Related to this issue has been the growth of restrictions and obstacles to non-citizens participating in research in cyber security and IT issues in general (e.g., greater difficulties in obtaining visas, and proposed changes to the deemed export rules on technology). This is counterproductive because many of the great advances made in the last few decades have come from foreign grad students in our universities, and from non-citizen engineers at companies and professors at universities who stayed in the US after getting their degrees. Historically, we have attracted the best and brightest researchers in the world to come study and pursue their academic and commercial dreams. If we continue to make the US an unfriendly destination for those individuals, other countries will reap the benefits of their inventiveness and intelligence.

The vast majority of vulnerabilities and risks to IT systems, whether within DoD or elsewhere, are plainly visible to people working in the field. Restricting who can address these vulnerabilities, or unduly classifying the results, will (in the usual case) only serve to limit our ability to protect ourselves.

I encourage members of the committee to carefully read the PITAC Cyber Security report. I participated in the research and writing of that report, and it goes into much more detail on the problems and issues behind our cyber security deficit.

Some Recommendations

There are several actions that can be taken to reduce the threat to Department of Defense IT systems. In the following two lists, I present some that I believe could have the most impact over the longer term. The first list is of items that Congress can address directly:

1. ***Most importantly,*** increase the priority and funding for scientific research into issues of security and protection of IT systems. This was the conclusion of the PITAC, and of numerous other studies cited in the PITAC report. Too much money is being spent on upgrading patches and not enough is being spent on fundamental research by qualified

personnel. There are too few researchers in the country who understand the issues of information security, and too many of them are unable to find funding to support fundamental research. This is the case at our military research labs, commercial labs, and at our university research centers. Increased spending for research is an investment in national defense and national economic competitiveness, and is not in the same category as many other expenditures for basic and applied research.

2. Increasingly, decisions on acquisition and deployment are being made by procurement officers rather than the individuals with better knowledge of the risks and needs for cyber defenses. At a minimum, there needs to be an explicit and prominent role kept for the designers and operators of systems to ensure that security needs are not trumped by arbitrary purchasing decisions.

3. Provide increased support to law enforcement for tools to track malware, and to support the investigation and prosecution of those who write malicious software and attack systems. This includes support for additional R&D for forensic tools and technologies.

4. Revisit laws, such as the DMCA (Digital Millennium Copyright Act), that criminalize technology instead of behavior. It is extremely counterproductive in the long run to prohibit the technologists and educators from building tools and studying threats when the “bad guys” will not feel compelled to respect such prohibitions.

The following list is comprised of suggestions that should be considered carefully by those within the military charged with ensuring cyber security and effectiveness of our forces.

1. Rethink the use of COTS products in mission-critical circumstances — the lowest cost is not necessarily the most fit for use. At the least, investigate better methods of screening and testing such products to ensure that they do not contain hidden, unwanted features.

2. Initiate significant research into the development of metrics for security and risk. Acquiring systems based on cost as the primary criterion is not reasonable for mission-critical applications. We need to be able to differentiate among different vendor solutions, and set standards of performance. Understandable metrics are needed for components and for entire systems of systems (although they are not sufficient on their own).

3. Emphasize the need for a systems-level view of information security. Assuring individual components does little to assure overall implementation and use. This requires trained personnel with an understanding of the “big picture” of IT security. Too often those who design and specify the systems do not understand how they are actually used....or misused.

4. Establish research into methods of better, more affordable software engineering, and how to build reliable systems from untrusted components. The military needs to reengage in this domain to ensure that their unique and critical needs are met.

5. Explicitly seek to create heterogeneous environments so that common avenues of attack are not present. This *may* require some extra expense *at first,* but eventually it may lead to increased compliance with standards, increased innovation, and increased choice in the marketplace, thus lowering costs while increasing security. If real standards (rather than *de facto* standards) are developed and followed, interoperability should not be a concern.

6. Complementary to the previous recommendation is giving thought to different architectures in appropriate circumstances that better meet policy objectives. For instance, rather than a computer on each desktop, thin-client technologies based on a mid-size computer in a

centralized location may provide all the same mission-critical services, but remove many of the dangerous aspects of distributed PCs. In this situation, patches need only be applied in one location, and there is a greatly reduced possibility of untrained users loading untested media or software.

7. Rethink the need to have all systems connected to a network. Standalone systems may not receive all of the latest patches as soon as they come out. However, that alacrity may not be needed as those systems can no longer be attacked over the network.

8. Reexamine the issues of the insider threat to mission critical systems – from obtaining software produced by uncleared personnel offshore and in this country, from using COTS products that are not designed for security and reliability, and from access and operation by untrained or unsupervised personnel. The intelligence community already does this, but it needs to be considered for wider use across the military.

9. Reexamine the automation of critical systems. Do we have adequate alternate methods of processing if core systems become unavailable or inaccessible? Do we have adequate non-computer copies of critical data that can be used operationally and to verify the integrity of online data? Have we automated a system that was flawed in the pre-automation form, and we have simply carried over the flaws into the new IT-based versions?

10. Establish better incentives for security. The current climate in many military commands and government agencies is to penalize operators for flaws, thus leading many of them to dread enhancement and exploration of better security.

Questions from the Committee

Given the category of threats, what is the worst case scenario to U.S. national security interests?

I am unsure what the worst case might be, but consider a time 15 years from now, where there is considerable international tension with a large country in Asia. Because of the underinvestment in long-term research in the US, we have been forced for the last several years to buy many of our advanced computing systems for the military and for civilian infrastructure control from companies located in that country. Outsourced maintenance is being done by companies in countries that are within the sphere of influence of this major country.

The tension increases, and our adversary invades a neighboring country – one of our long term allies. As that happens, large portions of our military command and control systems start crashing mysteriously, our databases of targeting information become corrupted, and some major logistics systems start issuing contradictory and incorrect orders for transportation and acquisition. Meanwhile our civilian power grid goes down, as does part of our communications. Outages randomly continue to occur for nearly a week including multiple failures in the SCADA systems. Hundreds die across the US from accidents and incidental problems. Some investigation suggests that these may be caused by hidden capabilities in the hardware and software of the controlling systems, but we don't have the tools or expertise to fully investigate the systems. The majority of our bases domestically do not have sufficient power to operate at capacity, and in any event, the lack of civilian power has taken out long-haul networks and satellite stations thus crippling our communications as well. What units are able to respond find that key data for targeting, command and control, and force protection are no longer correct or available, and no immediately usable backup systems are available.

The President decided to respond with limited, precision military force to the invasion of our ally, but the military is unable to mount a coordinated response because of the disruptions. By the time some order is restored, our ally has fallen. We have lost an ally, other allies have lost faith in us, and we have lost confidence in our own systems. Our economy has taken a major hit from the national power and telecommunication outages and the public is both fearful and angry. We receive an indirect message through third parties suggesting that if we don't accept our adversary's new "province" then the US might experience even worse mysterious outages affecting power, transportation, and finance. The military cannot protect us against these threats.

This case could be made even worse if it occurred simultaneously with a natural disaster or military attack (or both!).

Given the category of threats, what are the most likely scenarios the U.S. might face?

In the near term, I expect we will continue to face more acts of vandalism, crime and espionage. These will continue to cost a great deal of time and money to address. The severity and number of these attacks will increase over time.

There are too many variables to project far into the future. However, some of the most effective attacks involve clandestine exfiltration of information, and subtle alteration of internal data and operations. Given the current state of the art and practice, we do not have strong assurances that we have not already been victimized by such attacks, and that such attacks will not succeed in the future.

Are those scenarios preventable by nonmilitary means? If so, by what means?

I have provided a list of suggestions, based on my experience and research, in the preceding section.

Can those scenarios be addressed/mitigated by nonmilitary means? If so, by what means?

Again, this is addressed by the earlier section.

What other government departments and agencies (federal, state, and local) are involved in addressing the scenarios? What roles do they play (lead, supporting) and what resources do they possess?

Because of the interconnection and interdependency of our networks and computing systems, the list of participating agencies and departments is quite large. Obvious lead agencies are DHS and the FBI. Perhaps less obvious but very important are NIST and the NSF for the roles that they play in supporting research and collaboration. The DOE, DOJ and NIH all have roles, as do the police and homeland security departments of each state.

The key insight to answer this question is that the problem is one of a multi-pronged threat: attacks by criminals, vandals, terrorists, anarchists, spies, and military agencies are all possible, and may not be distinguishable before, during or after they occur. Additionally, those attacks may be specific or indiscriminate, and they are likely to be committed against civilian as well as military targets.

To effectively defend the nation, we need to continually invest and promote R&D into both short term and long term defenses for all sectors; we must obtain and deploy systems appropriate to their mission, without undue functionality, and chosen for robustness rather than cost; we must effectively investigate and prosecute misuse when it occurs to discourage other misuse and keep the "noise" low; and we must continue to understand that all our systems are interconnected and vulnerable.

What kinds of military capabilities are useful for addressing the threat? (The panel should identify two or three alternatives.)

I am unable to think of a military capability that will be adequate to deal with a decentralized network-centric attack by a non-national entity.

Which of these capabilities does the United States currently possess? Which of these capabilities is the United States currently developing? (Qualitative)

I do not have enough information to properly answer this question.

We are badly underinvested in long-term research for defenses, and we are badly undercapitalized in the area of investigation and forensics.

What military capabilities does the United States possess in sufficient quantity to address the threat? What military means does the United States have an excess of to address the threat? (Quantitative)

I believe my answers above address this question.

What other question(s) should be asked?

I believe my other responses address this question.

Conclusion

1. I will conclude this testimony by reiterating the concluding statement made in my testimony before a subcommittee of this committee on the 24th of July, 2003:

   > It is clear that we have deficiencies in our cyber defenses. Malicious and incorrect software pose particular threats because of their asymmetric potential — small operators can exercise large and devastating attacks on our defenses. The situation cannot be remedied simply by continuing to spend more on newer models of the same systems and defenses that are currently deficient. It will require vision and willingness to make hard choices to equip our military with the defensible IT systems they deserve.

I will be happy to expand on any of these points, now or in the future.

Thank you again for the opportunity to testify.

Acknowledgments

I received many suggestions from colleagues when composing this testimony. I wish to acknowledge the people listed for their assistance. However, the content and opinions expressed are my own, and the presence of these names should not be construed as endorsement of any of the statements herein: Annie Antón, William Arbaugh, Randy Bond, Carla Brodley, Charles Brownstein, Simson Garfinkel, Tim Grance, Peter Harsha, Peter Neumann, Ken Olthoff, David Padgham, Dan Reed, and Robin Roberts.