

# What Should the Department of Defense's Role in Cyber Be?

Testimony to House Armed Services Committee Subcommittee on Emerging Threats and Capabilities, 11 February 2011

Shari Lawrence Pfleeger

Director of Research, Institute for Information Infrastructure Protection  
Dartmouth College, Hanover, New Hampshire

Many thanks to the Subcommittee for inviting me to address these important questions. I am the Director of Research for the Institute for Information Infrastructure Protection, at Dartmouth College. The I3P is a consortium of 27 American universities, national laboratories, and non-profits focused on tackling problems in cyber security, dependability, safety and reliability. However, my opinions today are my own, not the I3P's, Dartmouth College's, nor my sponsors'.

I have organized my comments so that they address the three important questions posed by the Subcommittee's invitation to me.

## What are the significant challenges facing the private sector, federal government and Defense Department in preparing for the defense of the nation's cyber infrastructure?

- **Diverse and distributed ownership.** Much of the nation's critical cyber infrastructure is privately owned, and the federal government, including the Defense Department, requires its uses in providing critical functions and services to the American public. For this reason, private enterprise must recognize its responsibility in providing secure and resilient infrastructure components. The government plays an essential role in encouraging or requiring private enterprise to find solutions that permit the nation's economic and social engines to function. However, traditional approaches such as service level agreements, reliability standards, and problem reporting are made more difficult by the diverse and distributed ownership of the cyber infrastructure. Moreover, the cyber infrastructure is constructed of many parts that were not originally designed to provide critical infrastructure capabilities; because many of the security-related parts are not the primary money-makers for their providers, there is often little incentive for the providers to put security concerns above functionality provision.
- **Appeal as a criminal tool.** Many criminals use the cyber infrastructure as a tool to perpetrate their crimes. This usage enables criminals to act more broadly, more quickly, and with more anonymity than with other technologies. It is important to address the increase in cyber crime and cyber attack without restricting the far-more-common legal uses of the cyber infrastructure.
- **Difficulty in quickly identifying and reacting to emergent behavior.** Cyber problems are usually emergent behaviors with high degrees of uncertainty about both cause and extent of effect. Consequently, the time between recognizing an abnormality,

understanding cause and effect, and selecting an appropriate reaction can sometimes be quite long. And there are significant risks in acting with insufficient information. The large service providers can often act quickly to spot and stop aberrant behavior, especially when a disruption in service or function is temporary and non-critical. But when the aberrant behavior's cause is not certain and involves possible responses with life-threatening or international diplomatic repercussions, decision-makers must take far more care in reducing the uncertainty surrounding cause and effect.

### **What policy, legal, economic and technical challenges are critical?**

- **Misaligned incentives.** Economics and behavioral science provide numerous examples of misaligned cyber security incentives. (See van Eeten and Bauer, 2008 for a summary.) For instance, an organization that chooses not to act securely can nevertheless be protected by the secure actions of others. (This phenomenon is called “herd immunity,” where someone is protected when enough others keep the level of “infection” down, or “free riding,” where investments by others allow someone without investment to benefit, too.) Similarly, many organizations underinvest in cyber security: they take no up-front preventive or mitigative measures, preferring instead to deal with cyber attacks when they happen, and expending resources to clean up the resulting mess. (Rowe and Gallaher 2006) Indeed, Kunreuther and Heal (2003) point out that when one organization takes protective measures, those steps can actually discourage others from making security investments. These misaligned incentives sometimes result in good business decisions that are at the same time very bad security decisions. And the bad outcomes do not always affect the organization behaving badly, or not for very long. For example, the Defense Department may experience a breach of personal information about its soldiers, perhaps due to a cyber security failure. The impact is felt by the soldiers and their families; the breach may not cost the Defense Department much to remedy, and the long-term impact to recruitment and soldier effectiveness may be negligible. Similar examples of short-term effect to reputation and stock price are documented in the cyber security economics literature.
- **The need for diversity.** Many researchers and practitioners have argued that technological diversity leads to more secure products and networks, (Geer et al. 2003) and several studies (for example, Danezis and Anderson 2005) suggest that systems composed of diverse resources perform better than those whose nodes have the same resource mix. However, for economic reasons (especially in terms of the cost of maintenance and support), organizations often prefer technological uniformity. Anderson and Moore (2008) point out how externalities such as market dominance and access to applications reduce diversity. Moreover, it is more difficult to assure diversity than it would seem. Knight and Leveson (1986) demonstrated that attempts at diverse design are often dashed because of commonality in the way we train our software engineers. Other diversity failures can emerge by chance, when lack of knowledge, system complexity,

and business confidentiality lead to architectures with unintended dependencies and unexpected points of failure.

- **Perceived lack of security choices compatible with organizational culture and goals.** Too often, decision-makers view security as an inhibitor of creativity and productivity rather than as an enabler. For example, my profile of a large, multi-national corporation under sustained cyber attack revealed that the corporate president refused to remove administrative privileges from all corporate computers for fear that it would inhibit employees' computational flexibility. (Pfleeger 2010) Other studies show similar problems, with practitioners disabling or avoiding security in order to “get their jobs done.” (See Sasse 2004 for a survey of these problems.)

### **What should the government do to address these challenges?**

- **Address cyber crime and cyber attacks the way other unwelcome behaviors are addressed.** The government should incentivize or require better breach, fraud and abuse reporting, much as the Federal Trade Commission and the Food and Drug Administration track consumer problems and adverse consequences. Similarly, data about the nature and number of cyber attacks should be reported consistently each year, so that sensible trend data can form the basis for effective preventive and mitigative actions. Currently, almost all states require breach reporting when personal information is revealed—a good first step at capturing much-needed data. Other countries, such as Britain and France, have mandatory public reporting of bank fraud by crime method; efforts could be instituted here in the U.S. by extending existing criminal statutes to include cyber crimes. Our current reliance on convenience surveys for information about cyber attack trends can be misleading; more careful sampling and more consistent solicitation of data are essential. Early attempts by the Bureau of Justice Statistics at capturing cyber crime data on a large scale with a careful sampling scheme (see Rantala, 2008) had significant drawbacks, as documented by Cook and Pfleeger (2010). It may be more useful to capture data in various ways for various purposes, but doing so consistently over the years so that trends can be analyzed; some of the common terminology, such as the CVE (common vulnerabilities and exposures) list, can be useful in this regard. Good cyber economic models, informed by these representative, consistent data, offer the opportunity to improve cyber security investments and our general understanding of cyber risk relative to other kinds of risk. (Rue and Pfleeger, 2009)
- **Extend liability statutes to cover cyber technology**, so that the creators and maintainers of cyber technology—just like other technology providers—are forced to take responsibility for its failure. The situation now in cyber is similar to that of automobiles in the 1960s. When a lack of car safety was made more visible, the government responded by making automobile companies more liable for their unsafe practices and products. And as with automobiles, a combination of manufacturer liability and economic

constructs (such as insurance) could encourage more secure cyber product design and implementation.

- **Insist on good systems engineering.** The government is a significant buyer of cyber technology, and its purchasing power can be put to use in two important ways. First, by keeping track of cyber-related failures (security and otherwise), the government can refuse to continue to deal with system providers whose products and services are demonstrably insecure, unsafe or undependable. The data gathered in this process have another purpose: they can inform subsequent requirements selection, design decisions, and testing strategies, so that errors made in earlier products are less likely to occur in later ones. Second, the government can insist that critical systems, not just software, must be accompanied by solid, up-to-date formal arguments describing why the systems are secure and dependable. Such arguments are used in other domains, such as nuclear power plant safety, and can easily be extended to cyber systems. (Pfleeger, 2005) Moreover, suppliers' formal arguments can be woven into the system integrator's security and dependability arguments, to show that supply chain issues have been addressed with appropriate levels of care and confidence.
- **Provide economic incentives to encourage "good hygiene"** in individual organizations. Such incentives can speed implementation of protocols (such as DNSSEC), applications and systems that are demonstrably more secure. The incentives should also include rewards for speedy correction of security problems and punishments for lax attention to such problems. There are both public and private precedents for such incentives, such as tax incentives and insurance discounts. Previous attempts at self-regulation have been distinctly unsuccessful; for instance, Edelman (2006) shows that less reputable companies are more likely to buy trust certificates than reputable ones.
- **Encourage research in key multi-disciplinary areas that often get short shrift.** Many security failures occur not because a problem has no solution but because the solution has not been applied. From failure to apply patches promptly to reluctance to thoroughly scrub a system for vulnerabilities, many system problems result from system designers' failure to acknowledge the user's perspective and proclivities. Behavioral science (including psychology and organizational behavior) and behavioral economics have significant potential to improve the security and dependability of the nation's cyber infrastructure. For example, we in the I3P are managing three such projects. The first, on leveraging behavioral science to improve cyber security, is performing a series of carefully-controlled experiments in actual business settings to determine the best ways to improve security awareness and incentivize "good security hygiene." The second, on privacy, is investigating how organizational and national culture influence privacy perception and related behaviors. The third seeks ways to incorporate the user's perspective in the specification, design and testing of cyber security products and services. In the short term, this type of research can improve adoption rates for security technology, thereby reducing the "attack surface" at which malicious attackers take aim.

In the longer term, this research can lead to a more resilient cyber infrastructure that users are eager to use correctly and safely.

## References

- Anderson, Ross and Tyler Moore, "The Economics of Information Security," *Science* (314:5799), October 2006, pp. 610-613.
- Anderson, Ross and Tyler Moore, "Information Security Economics and Beyond," *Proceedings of the Information Security Summit 2008*, available at [http://www.cl.cam.ac.uk/~rja14/Papers/econ\\_czech.pdf](http://www.cl.cam.ac.uk/~rja14/Papers/econ_czech.pdf)
- Cook, Ian P. and Shari Lawrence Pfleeger, "Security Decision Support Challenges in Data Collection and Use," *IEEE Security & Privacy* 8(3), May 2010, pp. 28-35.
- Danezis, George and Ross Anderson, "The Economics of Resisting Censorship," *IEEE Security & Privacy*, 3(1), January 2005, pp. 45-50.
- Edelman, Benjamin, "Adverse Selection in Online 'Trust' Certifications," *Fifth Workshop on the Economics of Information Security*, 2006, available at <http://www.benedelman.org/publications/advsel-trust.pdf>
- Geer, Daniel, Charles P. Pfleeger, Bruce Schneier, John S. Quarterman, Perry Metzger, Rebecca Bace and Peter Gutmann, *CyberInsecurity: The Cost of Monopoly*, Computer & Communications Industry Association Report, September 24, 2003, available at <https://www.schneier.com/essay-318.html>
- Knight, John C. and Nancy G. Leveson, "An Experimental Evaluation of the Assumption of Independence in Multi-version Programming," *IEEE Transactions on Software Engineering*, SE-12(1), January 1986, pp. 96-109.
- Kunreuther, Howard and Geoffrey Heal, "Interdependent Security," *Journal of Risk and Uncertainty*, 26(2-3), March-May 2003, pp. 231-249.
- Pfleeger, Shari Lawrence, "Soup or Art? The Role of Evidential Force in Empirical Software Engineering" *IEEE Software*, January/February 2005.
- Pfleeger, Shari Lawrence, "Anatomy of an Intrusion," *IT Professional* 12(4), July 2010, pp. 20-28.
- Rantala, Ramona R., *Cybercrime Against Businesses, 2005*, Bureau of Justice Statistics Special Report NCJ 221943, September 2008, available at <http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf>.

Rowe, Brent and Michael Gallaher, "Private Sector Cyber Security Investment Strategies: An Empirical Analysis," Workshop on the Economics of Information Security, 2006, available at <http://weis2006.econinfosec.org/docs/18.pdf>

Rue, Rachel and Shari Lawrence Pfleeger, "Making the Best Use of Cybersecurity Economic Models," *IEEE Security & Privacy* 7(4), July 2009, pp. 52-60.

Sasse, M. Angela, "Usability and Trust in Information Systems," Cyber Trust and Crime Prevention Project, 2004, available at [http://hornbeam.cs.ucl.ac.uk/hcs/publications/Sasse\\_Usability%20and%20trust%20in%20information%20systems\\_Cyber%20Trust%20&%20Crime%20Prevention%20Project2004.pdf](http://hornbeam.cs.ucl.ac.uk/hcs/publications/Sasse_Usability%20and%20trust%20in%20information%20systems_Cyber%20Trust%20&%20Crime%20Prevention%20Project2004.pdf)

van Eeten, Michel J.G. and Johannes M. Bauer, *Economics of Malware: Security Decisions, Incentives and Externalities*, STI Working Paper JT03246705, OECD, 29 May 2008.