Statement of Jim Harper
Director of Information Policy Studies
The Cato Institute
to the
United States House of Representatives
Committee on Science and Technology
Subcommittee on Technology & Innovation
at a Hearing Entitled
"Assessing Cybersecurity Activities at NIST and DHS"

June 25, 2009

Executive Summary

Cybersecurity is a bigger, more multi-faceted problem than the government can solve, and it certainly cannot solve the whole range of cybersecurity problems quickly.

With a few exceptions, cybersecurity is less urgent than many commentators allege. There is no argument, of course, that cybersecurity is not important.

The policy of keeping true critical infrastructure off the public Internet has been lost in the "cybersecurity" cacophony. It is a simple security practice that will take care of many threats against truly essential assets.

The goal of policymakers should be not to solve cybersecurity, but to determine the systems that will best discover and propagate good security technology and practices.

As a market participant, the federal government is well positioned to effect the cybersecurity ecology positively, with NIST standards integral to that process. The federal government may also advance cybersecurity by shifting risk to sellers of technology by contract.

For the market failure that is on exhibit when insecure technology harms networks or other users, liability is preferable to regulation for discovering who should bear responsibility.

When the federal government abandons its role of market participant and becomes a market dominator, regulator, "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars.

Introduction

Chairman Wu, Ranking Member Smith, and members of the subcommittee, thank you for inviting me to address you in this hearing on the cybersecurity activities of the National Institute of Standards and Technology and the Department of Homeland Security. The hearings you have conducted so far are a valuable contribution to the national discussion, as I hope my participation in this hearing will be valuable as well.

My name is Jim Harper and I am director of information policy studies at the Cato Institute. In that role, I study and write about the difficult problems of adapting law and policy to the challenges of the information age. I also maintain an online federal spending resource called *WashingtonWatch.com*. Cato is a market liberal, or libertarian, think-tank, and I pay special attention to preserving and restoring our nation's founding, constitutional traditions of individual liberty, limited government, free markets, peace, and the rule of law.

I serve as an advisor to the Department of Homeland Security on its Data Integrity and Privacy Advisory Committee, and my primary focus in general is on privacy and civil liberties. I am not a technologist or a cybersecurity expert, but a lawyer familiar with technology and security issues. As a former committee counsel in both the House and Senate, I also blend an understanding of lawmaking and regulatory processes with technology and security. I hope this background and my perspective enhance your consideration of the many challenging issues falling under the name "cybersecurity."

In my testimony, I will spend a good deal of time on fundamental problems in cybersecurity and the national cybersecurity discussion so far. I will then apply this thinking to some of the policies NIST, DHS, and other agencies are working on.

The Use and Misuse of "Cyberspace" and "Cybersecurity"

One of the profound challenges you face in setting "cybersecurity" policy is the framing of the issue. "Cyberspace" is insecure, we all believe, and by making it integral to our lives, we are importing insecurity, as individuals and as a nation.

In some senses this is true, and "securing cyberspace" is a helpful way of thinking about the problem. But it also promotes overgeneralization, suggesting that a bounded set of behaviors called "cybersecurity" can resolve things.

A new world or "space" is indeed coming into existence through the development of communications networks, protocols, software, sensors, commerce, and content. In many ways, this world is distinct and different from the physical space that we occupy. In "cyberspace," we now do many of the things we used to do only in physical space: we shop, debate, read the news, work, gossip, manage our financial affairs, and so on.

Businesses and government agencies, of course, conduct their operations in the new "cyberspace" as well.

It is even helpful to extend this analogy and imagine "cyberspace" as organized like the physical world. Think of personal computers as people's homes. Their attachments to the network analogize to driveways, which connect to roads and then highways. (Perhaps phones and handheld devices are data-bearing cars and motorcycles.) Emails, financial files, and pictures are the personal possessions that could be stolen out of houses and private vehicles, leading to privacy loss.

Corporate and government networks are cyberspace's office buildings. Business data, personnel files, and intellectual property are the goods that sometimes get left on the loading dock, personnel files and business places that are left on the desk in an executive's office overnight, and so on. They can be stolen from the "office buildings" in data breaches.

How do you secure these places and things from theft, both casual and organized? How do you prevent fires, maintain water and electric service, ensure delivery of food, and prevent outbreaks of disease? How do you defend against military invasion or weapons of mass destruction in this all-new "space"?

These problems are harder to solve in some senses, and not as hard to solve in others. Consider, for example, that the "houses" and "office buildings" of cyberspace can be reconstituted in minutes or hours if software and data have been properly backed up. Lost possessions can be "regained" just as quickly—though copies of them may permanently be found elsewhere. "Cyberspace" has many resiliencies that real space lacks.

On the other hand, "diseases" (new exploits) multiply much more quickly and broadly than in the real world. "Cyber-public-health" measures like mandated vaccinations (the required use of security protocols) are important, though they may be unreliable. On a global public medium like the Internet, they would have to be mandated by an authority or authorities with global jurisdiction and authority over every computing device, which is unlikely and probably undesirable.

The analogy between cyberspace and real space shows that "cybersecurity" is not a small universe of problems, but thousands of different problems that will be handled in thousands of different ways by millions of people over the coming decades. Securing cyberspace means tackling thousands of technology problems, business problems, economics problems, and law enforcement problems.

In my opinion, if it takes decades to come up with solutions, that is fine. The security of things in "real" space has developed in an iterative process over hundreds and, in some cases, thousands of years. Even "simple" security devices like doors, locks, and windows

involve fascinating and intricate security, utility, and convenience trade-offs that are hard even for experts to summarize.

Many would argue, of course, that we do not have decades to figure out cybersecurity. But I believe that, with few exceptions, most of these assertions are mistaken. Your ability to craft sound cybersecurity policies for the government is threatened by the breathlessness of public discussion that is common in this field.

Calm Down, Slow Down

Overuse of urgent rhetoric is a challenge to setting balanced cybersecurity policy. Threat exaggeration has become boilerplate in the cybersecurity area, it seems, and while cybersecurity is important, overstatement of the problems will promote imbalanced responses that are likely to sacrifice our wealth, progress, and privacy.

For example, comparisons between "cyberattack" and conventional military attack are overwrought. As one example (which I select only because it is timely), the Center for a New American Security is hosting a cybersecurity event this week, and the language of the invitation says: "[A] cyberattack on the United States' telecommunications, electrical grid, or banking system could pose as serious a threat to U.S. security as an attack carried out by conventional forces."[1]

As a statement of theoretical extremes, it is true: The inconvenience and modest harms posed by a successful crack of our communications or data infrastructure could be more serious than an invasion by an ill-equipped, small army. But as a serious assertion about real threats, an attack by conventional forces (however unlikely) would be entirely more serious than any realistic cyberattack. We would stand to lose national territory, which cannot be reconstituted by rebooting, repairing software, and reloading backed-up files.

The Center for Strategic and International Studies' influential report, *Securing Cyberspace for the 44th Presidency*, said similarly that cybersecurity "is a strategic issue on par with weapons of mass destruction and global jihad."[2] Many weapons of mass destruction are less destructive than people assume, and the threat of global jihad appears to be waning, but threats to our communications networks, computing facilities, and data stores pale in comparison to true WMD like nuclear weapons. Controlling the risk of nuclear attack remains well above cybersecurity in any sound ranking of strategic national priorities.

---

[1] Center for a New American Security, "Developing a National Cybersecurity Strategy" web page (visited June 23, 2009) http://www.cnas.org/node/2818.

[2] CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," p. 15 (2008) http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf [hereinafter "CSIS Report"].

It is a common form of threat exaggeration to cite the raw number of attacks on sensitive networks, like the Department of Defense's. It suffers hundreds of millions of attacks per year. But happily most of these "attacks" are repetitious use of the same attack. They are mounted by "script kiddies"—unsophisticated know-nothings who get copies of others' attacks and run them on the chance that they will find an open door.

The defense against this is to continually foreclose attacks and genres of attack as they develop, the way the human body develops antibodies to germs and viruses. Securing against these attacks is important work, and it is not always easy, but it is an ongoing, stable practice in network management and a field of ongoing study in computer science. The attacks may continue to come in the millions, but this is less concerning when immunities and failsafes are in place and continuously being updated.

In his generally balanced speech on cybersecurity, President Obama cited a threat he termed "weapons of mass disruption."[3] Again, analogy to the devastation that might be done by nuclear weapons is misleading. Inconvenience and disruption are bad things, they can be costly, and in the extreme case deadly—again, cybersecurity is important—but securing against the use of real weapons on the U.S. and its people is a more important government role.

In a similar vein, a commentator on the National Journal's national security experts blog recently said, "Cyberterrorism is here to stay and will grow bigger."[4] Cyberterrorism is not here, and thus it is not in a position to stay.

Provocative statements of this type lack a key piece of foundation: They do not rest on a sound strategic model whereby opponents of the United States and U.S. power would use the capabilities they actually have to gain strategic advantage.

Take cyberterrorism. With communications networks, computing infrastructure, and data stores under regular attack from a variety of quarters—and regularly strengthening to meet them—it is highly unlikely that terrorists can pull off a cybersecurity event disruptive enough to instill widespread fear of further disruption. Fear is a necessary element for terrorism to work its will, of course. The impotence of computer problems to instill fear renders "cyberterrorism" an unlikely threat. This is not to deny the importance of preventing the failure of infrastructure, of course.

Cyberattacks by foreign powers have a similarly implausible strategic logic. The advantage gained by a disabling attack on private and civilian government infrastructure would be largely economic, with perhaps some psychological effects. Such attacks would not plausibly "soften up" the United States for invasion. But committing such attacks

---

[3] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[4] http://security.nationaljournal.com/2009/06/how-can-cyberspace-be-protecte.php

would risk harsh responses if the perpetrators were found, and conventional intelligence methods are undoubtedly keenly tuned to doing so. Ultimately, a foreign government's cyberattack on the United States would have to be a death-blow, as it would risk eliciting ruinous responses. This makes it very unlikely that a cyberattack on civilian infrastructure would be a tool of true war.

Attacking military communications infrastructure and data does have a rational strategic logic, of course. And the testimony your committee received from Dr. Leheny of the Defense Advanced Research Project Agency at your June 16 hearing illustrates some of what the Defense Department is doing to anticipate and prevent attacks on this true critical infrastructure.

The more plausible strategic use of attacks on communications and data infrastructure is not "cyberterrorism" or "cyberattack," but what might be called "cybersapping": Infiltrating networks to gain business intelligence, intellectual property, money, personal and financial data, and perhaps strategic government information. These infiltrations can slowly degrade the advantages that the U.S. economy and government have over others. They are important to address diligently and promptly. But they are not a reason to panic and overreact.

A final example of cybersecurity boilerplate that deserves mention is the alleged weakness of military information systems. The story that confidential files about the Joint Strike Fighter were compromised earlier this year has become a standard dire warning about our national vulnerability. But many are conveniently forgetting the other half of the story, even though it is available right there in some of the earliest reporting. According to a contemporaneous story on CNN.com:

> [O]fficials insisted that none of the information accessed was highly sensitive data. The plane uses stealth and other highly sensitive electronic equipment, but it does not appear that information on those systems was compromised, because it is stored on computers that are not connected to the Internet, according to the defense officials.[5]

The compromise of some data about the Joint Strike Fighter is regrettable, but this is also a story of cybersecurity success. The key security policy of keeping the most sensitive data away from the public Internet successfully protected that data. The Department of Defense deserves credit for instituting and maintaining that policy.

Cybersecurity is important, but exaggerating threats and failures as a matter of routine will lead to poor policymaking. Do not let the urgency of many statements about cybersecurity "buffalo" you into precipitous, careless, and intrusive policies.

---

[5] Mike Mount, "Hackers Stole Data on Pentagon's Newest Fighter Jet," CNN.com (Apr. 21, 2009) http://www.cnn.com/2009/US/04/21/pentagon.hacked/index.html.

Exhortation about some cybersecurity policies seem to be pushing others off the table, like the policy so successful at protecting the most important information about the Joint Strike Fighter. The simple, elegant policy of keeping truly critical infrastructure off the public Internet is not receiving enough discussion.

Critical Infrastructure: Off the Internet

At the confirmation hearing of Commerce Secretary Gary Locke earlier this year, Senator Jay Rockefeller stated his view of the cybersecurity problem in no uncertain terms. Of cyberattack, he said:

> It's an act which can shut this country down—shut down its electricity system, its banking system, shut down really anything we have to offer. It is an awesome problem. . . . It is a fearsome, awesome problem.[6]

What is fearsome is the embedded premise that everything important to our country would be put on the Internet rather than controlled over separate, dedicated networks. This is not true, as the example of the Joint Strike Fighter example illustrates. And it turns out that many important functions in government and society are indeed handled by dedicated communications networks.

Cato Institute adjunct fellow Timothy B. Lee, a Ph.D. student in computer science at Princeton University and an affiliate of the Center for Information Technology Policy, commented on the Estonian cyberattacks last year:

> [S]ome mission-critical activities, including voting and banking, are carried out via the Internet in some places. But to the extent that that's true, the lesson of the Estonian attacks isn't that the Internet is "critical infrastructure" on par with electricity and water, but that it's stupid to build "critical infrastructure" on top of the public Internet. There's a reason that banks maintain dedicated infrastructure for financial transactions, that the power grid has a dedicated communications infrastructure, and that computer security experts are all but unanimous that Internet voting is a bad idea.[7]

Tim has also noted that the Estonia attacks did not reach parliament, ministries, banks, and media—just their Web sites. Access to some businesses and government agencies went down, but their core functions were not compromised.

Yet this policy—of keeping critical functions away from the Internet—has received almost no discussion in the recent major reports on cybersecurity. The White House's

---

[6] *See* "Jay Rockefeller: Internet Should Have Never Existed," YouTube (posted Mar. 20, 2009) http://www.youtube.com/watch?v=Ct9xzXUQLuY.

[7] Tim Lee, "The Internet Isn't 'Critical Infrastructure,'" TechDirt (May 27, 2008) http://www.techdirt.com/articles/20080522/1905471205.shtml

Cyberspace Policy Review did not highlight this approach,[8] and the President's speech presenting the review did not either. The CSIS report also did not emphasize this simple, straightforward method for securing truly critical functions.

Where security is truly at a premium, the lion's share of securing infrastructure against cyberattack can be achieved by the simple policy of fully decoupling it from the Internet.

"Criticality" has become a popular line to draw in discussions of cybersecurity, of course, and the meaning of the term is in no way settled. A 2003 Congressional Research Service report explored the dimensions of the concept at the time.[9] My study of "criticality" is cursory, but the CSIS report's suggestion is sensible, if loosely drawn:

> [C]ritical means that, if the function or service is disrupted, there is immediate and serious damage to key national functions such as U.S. military capabilities or economic performance. It does not mean slow erosion or annoying disruptions.[10]

In my mind, criticality should probably turn on whether compromise of the resource would immediately and proximately endanger life and health. Immediacy is an important limitation because resources that can be promptly repaired to prevent harm should be made resilient that way rather than treated as critical infrastructure.

Proximity to harm is also important to prevent "criticality" grade-inflation. The loss of electric power for even an hour will kill people on respirators in hospitals, for example, but the proximate solution to such foreseeable risks is to have backup power systems at hospitals—not to make the entire electricity grid critical infrastructure on that basis.

If it is to be a focal point for cybersecurity policies, the notion of "critical infrastructure" must be sharply circumscribed. Given the special treatment accorded critical infrastructure by government, private entities will all clamor for that status, and the government will be stuck protecting thousands of things that are kind of important, rather than the networks and data that are immediately needed for protecting life and health.

Keeping the small universe of truly critical infrastructure entirely separate from the public Internet, and encouraging private operators of critical infrastructure to do so, is a policy that has not received enough discussion so far. It deserves a great deal more.

---

[8] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," The White House (undated) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/..

[9] John Moteff et al., Resources, Science, and Industry Division, Congressional Research Service, "Critical Infrastructures: What Makes an Infrastructure Critical?", CRS Order Code RL31556 (updated Jan. 29, 2003) http://www.fas.org/irp/crs/RL31556.pdf.

[10] CSIS Report, p. 44.

But this is one among dozens of policy choices to deal with thousands of problems. The many complex challenges lumped together as "cybersecurity" cannot be solved by any one expert, group of experts, legislature, regulatory body, or commission. It has too many moving parts.

Rather than trying to address cybersecurity in toto, I recommend addressing the problem at a level once-removed: By asking what systems we should use to address cybersecurity. There are a variety of social mechanisms, each with merits and demerits.

Cybersecurity Through Contract

In my testimony so far, I have argued against over-generalization and over-heated rhetoric around cybersecurity. Cybersecurity is many different problems, only some of which are urgent.

None of this is to deny that cybersecurity is a serious and important challenge. I applaud the work of the Defense Department to secure its critical information, and find very interesting DARPA's innovative work to develop networks over which our military branches can conduct their very important functions. These are two examples among many government-wide efforts to secure true critical infrastructure.

But what about the rest of the country's communications and data infrastructure? Is the entire nation's cyberstuff a "strategic national asset," as the president suggested in his speech on cybersecurity?[11] Should it all come under a military or quasi-military command-and-control operation?

The CSIS study called for a "comprehensive national security strategy for cyberspace" and stated accordingly and unflinchingly that the government should "regulate cyberspace."[12] The report also laid our cybersecurity woes at the feet of the market: "We have deferred to market forces in the hope that they would produce enough security to mitigate national security threats. It is not surprising that . . . industrial organization and overreliance on the market has not produced success."[13]

Competition and markets should not be passed over in favor of regulation. Indeed, the argument for regulation begs the central question: What do we want from our technical infrastructures so that we have appropriate security? What would a cybersecurity regulation *say*? Nobody yet knows.

---

[11] "Remarks by the President on Securing Our Nation's Cyber Infrastructure," (May 29, 2009) http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.
[12] CSIS Report, pp. 1-2.
[13] CSIS Report, p. 12.

To illustrate, FISMA the Federal Information Security Management Act, has not taken care of cybersecurity for the federal government. Federal chief information security officers and others rightly criticize the government's self-regulation for its focus on compliance reporting and paperwork at the expense of addressing known problems.[14]

If the federal government knew how to do cybersecurity well, FISMA would be a to-do list that more or less secured the federal enterprise. We would not have the cybersecurity problem all agree we have. But the practices that lead to successful cybersecurity have not yet been discovered. Regulations to implement these undiscovered practices would not help.

Success in cybersecurity is not easy to define. Professor Ed Felten from Princeton University's Center for Information Technology Policy points out that the ideal is not perfect security, but optimal security—the efficient point where investments in security avoid equal or greater losses.[15] Communications and computing devices are meant to process, display, and transmit information that they often acquire from other resources. To make them useful, we must embrace the risk of opening them up to other computers, software, and data. Some level of insecurity is what makes the Internet, computing, and "cyberspace" so useful and valuable.

Again, the question is what processes we can use to discover optimal or near-optimal cybersecurity products and behaviors, then propagate them throughout the society.

Criticisms of the market are not misplaced, though they may be mis-focused. The market for communications and computing technologies is very immature. Many products are rushed to market without adequate security testing. Many are delivered with insecure settings enabled by default. My impression also is that most are sold without any warranty of fitness for the purposes users will put them to, leaving all risk of failure with buyers who are poorly positioned to make sound security judgments. There are several ways to address these problems.

As this committee is aware, the federal government is one of the largest purchasers—if not the largest purchaser—of information technology in the world. This is not the preferred state of affairs from my perspective, but there is no reason to deny that its purchasing decisions can affect the improvement of products available on the market.

Thanks to entities like the National Institute of Standards and Technology, the federal government is also one of the most sophisticated purchasers of technology. As other witnesses and advocates have articulated better than I can, the government can drive

---

[14] *See, e.g.,* Government Futures, "The 2009 State of Cybersecurity from the Federal CISO's Perspective — An (ISC)2 Report" (April 2009) http://media.haymarketmedia.com/Documents/7/FederalCISOSurveyReport_1638.pdf.

[15] Nestor Abreu, "Conversation: Debugging our Cyber-Security Policy" (podcast at minute 12:00) (Feb. 27, 2009) http://citp.princeton.edu/blog/2009/02/27/conversation-debugging-our-cyber-security-policy/.

maturation in the market for technology products by setting standards and defaults for the products and services it buys.

The federal government can also insist on shifting the risk of loss from the buyer to the seller. Contracts with technology sellers can include guarantees that their products are fit for the purposes to which they will be put—including, of course, secure operation.

Federal buyers should expect to pay more if they demand fitness and security guarantees, of course, but more secure products have more value. Sellers will have to do more thorough development and more rigorous security testing. Because they currently bear little or no risk of loss, technology sellers will probably howl at the prospect of bearing risk, but ready to step in will be technology sellers willing to produce better, more secure, and more reliable products for the premium that gets them.

As a large market participant, the federal government can have a good influence on the security ecology without resorting to intrusive regulation. Whether it creates a "gold standard" for security in technologies purchased in the private sector, or whether it moves the market toward contract-based liability for technology sellers, the federal government can help the technology market mature.

Cybersecurity Through Tort Liability

There is more to criticism of the market for cybersecurity than "lack of maturity," however. There is also an arguable market failure in the area of technology products and services, caused by a lack of maturity in the law. I was pleased that the executive summary of the White House *Cyberspace Policy Review* cited a short paper I wrote arguing that updated tort law would be superior to regulation for curing the market.[16]

A market failure exists when the market price of a good does not include the costs or benefits of externalities (harmful or beneficial side effects that occur in the production, distribution, or consumption of a good). Producers or consumers may have little incentive to alter activities that contribute to air pollution, for example, when the costs of pollution do not affect their costs. Likewise, users of computers that are insecure may harm the network or other users, such as when malware infects a computer and uses it to launch spam or distributed denial-of-service attacks.

When there is no contractual relations between the parties, getting network operators, data owners, and computer users to internalize risks can be done one of two ways: Regulation—you mandate certain behaviors—or liability—you make them pay for harms they cause others. Regulation and liability each have strengths and weaknesses, but I believe a liability regime is ultimately superior.

---

[16] Much of Jim Harper, "Government-Run Cyber Security? No, Thanks," Cato Institute TechKnowledge #123 (March 13, 2009) http://www.cato.org/tech/tk/090313-tk.html, is incorporated into this testimony.

One of the main problems with regulation—especially in a dynamic field like technology—is that it requires a small number of people to figure out how things are going to work for an unknown and indefinite future. Those kinds of smarts do not exist.

So regulators often punt: When the Financial Services Modernization Act tasked the Federal Trade Commission with figuring out how to secure financial information, it did not do that. Instead, the "Safeguards Rule"[17] (similarly to FISMA) simply requires financial institutions to have a security plan. If something goes wrong, the FTC will go back in and either find the plan lacking or find that it was violated.

Another weakness of regulation is that it tends to be too broad. In an area where risks exist, regulation will ban entire swaths of behavior rather than selecting among the good and bad. In 1998, for example, Congress passed the Children's Online Privacy Protection Act, and the FTC set up an impossible-to-navigate regime for parental approval of the websites their children could use.[18] Today, no child has been harmed by a site that complies with COPPA because they are so rare. The market for serving children entertaining and educational content is a shadow of what it could be.

Regulators and regulatory agencies are also subject to "capture." Industries have historically co-opted the agencies intended to control them and turned those agencies toward insulating incumbents from competition.[19]

And regulation often displaces individual justice. The Fair Credit Reporting Act preempted state law causes of action against credit bureaus that, thus, cannot be held liable for defamation when their reports wrongfully cause someone to be denied credit. "Privacy" regulations under the Health Insurance Portability and Accountability Act gave enforcement powers to an obscure office in the Department of Health and Human Services. While a compliance kabuki dance goes on overhead, people who have suffered privacy violations are diverted to seeking redress by the grace of a federal agency.

Tort liability is based on the idea that someone who does harm, or allows harm to occur, should be responsible to the injured party. The role of law and government is to prevent individuals from harming one another. When a person drives a car, builds a building, runs a hotel, or installs a light switch, he or she owes it to anyone who might be injured to keep them safe. A rule of this type could apply to owners and operators of networks and databases, and possibly even to software writers and computer owners.

---

[17] *See* Federal Trade Commission, "Protecting Customers' Personal Information: The Safeguards Rule" web page (visited June 23, 2009) http://www.ftc.gov/bcp/edu/microsites/idtheft/business/safeguards.html.
[18] *See* Federal Trade Commission, "You, Your Privacy Policy, and COPPA: How to Comply with the Children's Online Privacy Protection Act" web page (visited June 23, 2009) http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus51.pdf.
[19] *See* Timothy B. Lee, "The Durable Internet: Preserving Network Neutrality without Regulation," Cato Policy Analysis #626 (Nov. 12, 2008) http://www.cato.org/pub_display.php?pub_id=9775.

A liability regime is better at discovering and solving problems than regulation. Owners faced with paying for harms they cause will use the latest knowledge and their intimacy with their businesses to protect the public. Like regulation, a liability regime will not catch a new threat the first time it appears, but as soon as a threat is known, all actors must improve their practices to meet it. Unlike regulations, which can take decades to update, liability updates automatically.

Liability also leaves more room for innovation. Anything that causes harm is forbidden, but anything that does not cause harm is allowed. Entrepreneurs who are free to experiment will discover consumer-beneficial products and services that improve health, welfare, life, and longevity.

Liability rules are not always crystal clear, of course, but when cases of harm are alleged in tort law, the parties meet in a courtroom before a judge, and the judge neutrally adjudicates what harm was done and who is responsible. When an agency enforces its own regulation, it is not neutral: Agencies work to "send messages," to protect their powers and budgets, and to foster future careers for their staffs.

Especially in the high-tech world of today, it is hard to prove causation. The forensic skill to determine who was responsible for an information-age harm is still too rare. But regulation is equally subject to evasion. And liability acts not through lawsuits won, but by creating a protective incentive structure.

One risk unique to liability is that advocates will push to do more with it than compensate actual harms. Some would treat the creation of risk as a "harm," arguing, for example, that companies should pay someone or do something about potential identity fraud just because a data breach created the risk of it. They often should, but blanket regulations like that actually promote too much information security, lowering consumer welfare as people are protected against things that do not actually harm them.

It is also true that the tort liability system has been abused in some cases. Plaintiffs' bars have sought to turn litigation into another regulatory mechanism—or a cash cow. State common law reforms to meet these challenges are in order; dismissing the common law out of hand is not.

There are dozens of complexities to how the tort law would operate in the cybersecurity area, of course. The common law is a system of discovery that crafts doctrines to meet emerging challenges. I cannot predict each challenge common law courts would encounter and how they would address them, but the growth of common law doctrines to prevent harm is an important alternative to the heavy hand of regulation.

As complex and changing as cyber security is, the federal government has no capability to institute a protective program for the entire country. While it secures its own networks, the federal government should observe the growth of state common law duties that

require network operators, data owners, and computer users to secure their own infrastructure and assets. (They in turn will divide up responsibility efficiently by contract.) This is the best route to discovering and patching security flaws in all the implements of our information economy and society.

Between the two, contract and tort liability can provide a seamless web of cybersecurity incentives, spreading risks to the parties most capable of controlling them and bearing their costs. Regulation pushes responsibility to protect where it is politically palatable, not where it is economically most efficient or best done. Regulation often shields the private sector from liability, foisting risk onto the public—one of the concerns I will turn to next.

Standards, Public-Private Partnerships, and the Risks Thereof

As a market participant, the federal government can play an important role in promoting secure products and practices. When it leaves the role of market participant and becomes a market dominator, a regulator, a "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars. I will address selected examples of NIST and DHS activity in that light.

As a standard-setting organization for the federal government, NIST is a valuable resource—not just for the government but for the cybersecurity ecology. But standards are tricky business. What may be appropriate in one context may not be in another

An area of keen interest to me as an advocate for privacy and civil liberties is the avoidance of a national ID system in the United States. My book, *Identity Crisis: How Identification is Overused and Misunderstood*, sought to reveal the demerits in having a U.S. national ID. The REAL ID Act of 2005, which attempted to create a national ID system in the United States, has foundered for a variety of reasons. Unfortunately, a bill recently introduced in the Senate would seek to revive this national ID program.[20]

Accurate identification or "identity security" is important in some contexts, but less so in others. Anonymity and obscurity are important protections for Americans' privacy and freedom to speak and act as they wish. Ultimately, I believe a diverse and competitive identity and credentialing system will deliver all the benefits that digital identity systems can provide, without the surveillance.

So I was concerned to see one bullet point in the testimony of Cita Furlani from NIST at your recent joint hearing. She characterized NIST's identity and credentialing

[20] S. 1261, The PASS ID Act (111th Cong., 1st Sess.) http://www.washingtonwatch.com/bills/show/111_SN_1261.html.

management standard for federal employees and contractors (FIPS 201) as "becoming the de facto national standard."[21]

It is unclear exactly what this means, of course, and I do not view FIPS 201 as the foremost threatened national ID standard at this time. But the needs in identity and credentialing outside the federal government are quite different from those within the government. The same market dominance that makes the federal government such a potential boon to cybersecurity could make it an equal bane to privacy and civil liberties should FIPS 201 be adopted widely by state governments for their employees, by states for their drivers' licenses and IDs, and in private-sector employment and access control. The same is probably true of other standards in other ways.

Cybersecurity standard-setting for federal government purchasing and use should present few problems. It can often be beneficial when it drives forward the cybersecurity marketplace. But pressing standards onto the private sector where they are not a good fit—in delicate areas such as personal information handling—creates concerns.

Professor Schneider from Cornell said it well in your first hearing of this series:

> [T]he Internet is as much a social construct as a technological one, and we need to understand what effects proposed technological changes could have; forgoing social values like anonymity and privacy (in some sense, analogous to freedom of speech and assembly) in order to make the Internet more trustworthy might significantly limit the Internet's utility to some, and thus not be seen as progress.[22]

A different array of concerns arises from nominal "public-private partnerships." The concept is much ballyhooed among governments and corporations because it suggests happiness and cooperation. But I am not enthusiastic about a joining of hands between the government and the corporate sector.

Public-private partnerships take many forms, of course. The least objectionable are information-sharing arrangements like the Department of Homeland Security's US-CERT, or United States Computer Emergency Readiness Team. But consumers, the

---

[21] Testimony of Ms. Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST), to a hearing entitled "Agency Response to Cyberspace Policy Review," Subcommittee on Technology & Innovation, Committee on Science and Technology, United States House of Represenatives, p. 4 (June 16, 2009) http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/16jun/Furlani_Testimony.pdf.

[22] Testimony of Dr. Fred B. Schneider, Samuel B. Eckert Professor of Computer Science, Cornell University, to a hearing entitled "Cyber Security R&D," Subcommittee on Technology & Innovation, Committee on Science and Technology, United States House of Representatives, p. 4 (June 10, 2009) http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Research/10jun/Scheider_Testimony.pdf.

society, and our economy do not get the best from corporations when they cooperate, much less when they cooperate with government. Markets squeeze the most out of the business sector when competitors are nakedly pitted against each other and forced to compete on every dimension of their products and services, including cybersecurity.

Programs like US-CERT run the risk of diminishing competition and innovation in cybersecurity. Vulnerability warning is not a public good; it can be provided privately by companies competing against each other to do the best job for their clients. "Free" taxpayer-funded vulnerability warning will tend to squeeze private providers out of the market.

This risks lowering overall consumer welfare, especially if it leads to cybersecurity monoculture. "Monoculture" is the idea that uniformity among security systems is a weakness. In a security monoculture, one flaw could be exploited in many domains at once, bringing them all down and creating problems that would not have materialized in a diverse security environment.

With US-CERT this is only a risk. Public-private partnerships of other stripes raise more powerful concerns.

Earlier in my testimony, I wrote about how liability can promote cybersecurity. It is equally the case that the absence of liability can degrade security. If public-private partnerships confuse lines of responsibility for security, the results can be very bad indeed.

Consider how responsibility for passenger air transportation was mixed before the 9/11 attacks. Airlines nominally provided security, but they had to obey the dictates of the Federal Aviation Administration. Were something bad to happen, both entities were in a position to deny responsibility.

Flying a plane into a building had been written about in a 1994 novel—and kamikaze attacks were, of course, a tactic of the Japanese in World War II—but on 9/11 hijacking protocols had not been seriously revamped since the 1970s, when absconding to Cuba was the chief goal of most airline takeovers.

After 9/11, neither airlines nor the Federal Aviation Administration shouldered responsibility. The airlines moved swiftly to capitalize on emotion and patriotism, getting Congress to shield them from liability, give them an infusion of taxpayer dollars, and take over their security obligations. This "public-private partnership" in security was a disaster from start to finish, and remains so. The party ultimately bearing the loss—and still at risk today—was the American taxpayer and traveler.

This illustration is not to suggest that cybersecurity failures threaten attacks equivalent to 9/11. It is simply to suggest that the better role of the government is to stand apart from

industry and to arbitrate liability when a company has failed to meet its contractual or tort-based obligations.

Public-private partnerships may also be conduits for transferring taxpayer funds to corporations, or to universities who do research for corporations. While reviewing the testimonies presented to you in earlier hearings, I was impressed by the nearly uniform requests for taxpayer money.

Much of the money requested would go to research that industry needs to do a good job. In other words, it is research they would fund themselves in the absence of a subsidy. Using a small amount of money taken from each taxpayer, Congress can give money to corporations and claim a role in the production of security, even though the corporations would have put their own money to that use themselves. This is another form of "partnership" where the American taxpayer loses.

When the federal government abandons the role of market participant and neutral arbiter, difficulties arise. Though NIST standards are useful for the federal government—and many of them can apply well in the private sector—they may not be appropriately forced on the private sector when the government is market-dominant. Government-corporate collaboration raises many risks: security monoculture; mixed responsibility and weakened security; and simple waste of taxpayer dollars.

Cybersecurity is special, but not so special that principles about the limited role of government should go by the wayside. We will get the best security and the best deal for taxpayers and the public if the government remains within its proper sphere.

Conclusion

Cybersecurity is a huge topic, and I have ranged widely across it in my imperfect testimony. I hope it is more clear that "cybersecurity" is a bigger, more multi-faceted problem than the government can solve, and government certainly cannot solve the whole range of cybersecurity problems quickly.

Happily, with a few exceptions, cybersecurity is also less urgent than many commentators allege. "Cyberattack" or "cyberterrorism" might be replaced by "cybersapping" of the country's assets and technology as the threat we should promptly and diligently address. There is no argument, of course, that cybersecurity is not important.

I am concerned that the policy of keeping true critical infrastructure off the public Internet has been lost in the cybersecurity cacophony. It is a simple, elegant practice that will take care of many threats against truly essential assets.

The government will not fix the nation's cybersecurity. Your goal as policymakers should be one level removed: to determine the system that will best discover and propagate good cybersecurity practices.

As a market participant, the federal government is well positioned to effect the cybersecurity ecology positively, with NIST standards integral to that process. The federal government may also advance cybersecurity by shifting risk to sellers of technology by contract.

For the market failure that is on exhibit when insecure technology harms networks or other users, liability is a preferable mechanism to regulation for discovering who should bear the responsibility to protect.

When the federal government abandons its role of market participant and becomes a market dominator, regulator, "partner," or investor with private sector entities, a number of risks arise, including threats to privacy and civil liberties, weakened competition and innovation, and waste of taxpayer dollars.

I appreciate the chance to share these ideas with you, and I hope that they will aid the committee's deliberations.

BOSTONREVIEW
JULY/AUGUST 2009

Cyber-Scare

The exaggerated fears over digital warfare

Evgeny Morozov

The age of cyber-warfare has arrived. That, at any rate, is the message we are now hearing from a broad range of journalists, policy analysts, and government officials. Introducing a comprehensive White House report on cyber-security released at the end of May, President Obama called cyber-security "one of the most serious economic and national security challenges we face as a nation." His words echo a flurry of gloomy think-tank reports. The Defense Science Board, a federal advisory group, recently warned that "cyber-warfare is here to stay," and that it will "encompass not only military attacks but also civilian commercial systems." And "Securing Cyberspace for the 44th President," prepared by the Center for Strategic and International Studies, suggests that cyber-security is as great a concern as "weapons of mass destruction or global jihad."

Unfortunately, these reports are usually richer in vivid metaphor—with fears of "digital Pearl Harbors" and "cyber-Katrinas"—than in factual foundation.

Consider a frequently quoted CIA claim about using the Internet to cause widespread power outages. It derives from a public presentation by a senior CIA cyber-security analyst in early 2008. Here is what he said:

We have information, from multiple regions outside the United States, of cyber-intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber-attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet.

So "there is information" that cyber-attacks "have been used." When? Why? By whom? And have the attacks caused any power outages? The CIA may have some classified information, but very little that is unclassified suggests that such cyber-intrusions have occurred.

Or consider an April 2009 *Wall Street Journal* article entitled "Electricity Grid in U.S. Penetrated By Spies." The article quotes no attributable sources for its starkest claims about cyber-spying, names no utility companies as victims of intrusions, and mentions

just one real cyber-attack, which occurred in Australia in 2000 and was conducted by a disgruntled employee rather than an external hacker.

It is alarming that so many people have accepted the White House's assertions about cyber-security as a key national security problem without demanding further evidence. Have we learned nothing from the WMD debacle? The administration's claims could lead to policies with serious, long-term, troubling consequences for network openness and personal privacy.

Cyber-security fears have had, it should be said, one unambiguous effect: they have fueled a growing cyber-security market, which, according to some projections, will¬†grow twice as fast as the rest of the IT industry. Boeing, Raytheon, and Lockheed Martin, among others, have formed new business units to tap increased spending to protect U.S. government computers from cyber-attacks. Moreover, many former government officials have made smooth transitions from national cyber-security policy to the lucrative worlds of consulting and punditry. Speaking at a recent conference in Washington, D.C., Amit Yoran—a former cyber-security czar in the Bush administration and currently the C.E.O. of NetWitness, a cyber-security start-up—has called hacking a national security threat, adding that "cyber-9/11 has happened over the last ten years, but it's happened slowly, so we don't see it." One way for the government to protect itself from this cyber-9/11 may be to purchase NetWitness's numerous software applications, aimed at addressing both "state and non-state sponsored cyber threats."

From a national security perspective, cyber-attacks matter in two ways. First, because the back-end infrastructure underlying our economy (national and global) is now digitized, it is subject to new risks. Fifty years ago it would have been hard—perhaps impossible, short of nuclear attack—to destroy a significant chunk of the U.S. economy in a matter of seconds; today all it takes is figuring out a way to briefly disable the computer systems that run Visa, MasterCard, and American Express. Fortunately, such massive disruption is unlikely to happen anytime soon. Of course there is already plenty of petty cyber-crime, some of it involving stolen credit card numbers. Much of it, however, is due to low cyber-security awareness by end-users (you and me), rather than banks or credit card companies.

Second, a great deal of internal government communication flows across computer networks, and hostile and not-so-hostile parties are understandably interested in what is being said. Moreover, data that are just sitting on one's computer are fair game, too, as long as the computer has a network connection or a USB port. Despite the "cyber" prefix, however, the basic risks are strikingly similar to those of the analog age. Espionage has been around for centuries, and there is very little we can do to protect ourselves beyond using stronger encryption techniques and exercising more caution in our choices of passwords and Wi-Fi connections.

To be sure, there is a war-related caveat here: if the military relies on its own email system or other internal electronic communications, it is essential to preserve this capability in wartime. Once more, however, the concern is not entirely novel; when radio

was the primary means of communication, radio-jamming was also a serious military concern; worries about radio go back as far as the Russo-Japanese War of 1904-1905.

Before accepting the demands of government agencies for new and increased powers, we should look more closely at well-defined dangers.

The ultimate doomsday scenario—think *Live Free or Die Hard*—could involve a simultaneous attack on economic e-infrastructure and e-communications: imagine al Qaeda disabling banks, destroying financial data, disrupting networks, and driving the American economy back to the nineteenth century. This certainly sounds scary—almost as scary as raptors in Central Park or a giant asteroid heading toward the White House. The latter two are not, however, being presented as "national security risks" yet.

There are certainly genuine security concerns associated with the Internet. But before accepting the demands of government agencies for new and increased powers to fight threats in cyberspace and prepare for cyber-warfare, we should look more closely at well-defined dangers and ask just where existing technological means and legal norms fall short. Because the technologies are changing so quickly, we cannot expect definitive answers. But cyber-skeptics—who argue that cyber-warfare is still more of an urban legend than a credible hazard—appear to be onto something important.

One kind of cyber-security problem grows out of resource scarcity. A network has only so much bandwidth; a server can serve only so much data at one time. So if you want to disable (or simply slow down) the computer backbone of a national economy, for example, you need to figure out how to reach its upper limit.

It would be relatively easy to protect against this problem if you could cut your computer or network off from the rest of the world. But as the majority of governmental and commercial services have moved online, we expect them to be offered anywhere; Americans still want to access their online banking accounts at Chase even if they are travelling in Africa or Asia. What this means in practice is that institutions typically cannot shut off access to their online services based on nationality of the user or the origin of the computer (and in the case of news or entertainment sites, they do not want to: greater access means more advertising income).

Together, these limitations create an opportunity for attackers. Since no one, not even the U.S. government, has infinite computer resources, any network is potentially at risk.

Taking advantage of this resource scarcity could be an effective way of causing trouble for sites one does not like. The simplest—and also the least effective—way of doing this is to visit the URL and hit the "reload" button on your browser as often (and for as long) as you can. Congratulations: you have just participated in the most basic kind of "denial-of-service" (DoS) attack, which aims to deny or delay the delivery of online services to legitimate users. These days, however, it would be very hard to find a site that would suffer any noticeable damage from such a nuisance; what is missing from your cyber-guerilla campaign is scale.

Now multiply your efforts by a million—distribute your attacks among millions of other computers—and this could be enough to cause headaches to the administrators of many Web sites. These types of attacks are known as “distributed denial-of-service” or DDoS attacks. Administrators may be able to increase their traffic and bandwidth estimates and allocate more resources. Otherwise they have to live with this harassment, which may disable their Web site for long periods.

DDoS attacks work, then, by making heavier-than-normal demands on the underlying infrastructure, and they usually cause inconvenience rather than serious harm. Not sure how to do it yourself? No problem: you can buy a DDoS attack on the black market. Try eBay.

In fact, your own computer may well be participating in a DDoS attack right now. You may, for example, have inadvertently downloaded a trojan—a hard-to-detect, tiny piece of software—that has allowed someone else to take control of your machine, without obvious effect on your computer’s speed or operations. Some computer experts put the upper limit of infected computers as high as a quarter of all computers connected to the Internet.

Because a single computer is inconsequential, the infected computers form “botnets”—nets of robots—that can receive directions from a command-and-control center—usually just another computer on the network with the power to give commands. What makes the latest generation of botnets hard to defeat is that every infected computer can assume the role of the command-and-control center: old-fashioned methods of decapitation do not work against such dispersed command-and-control. Moreover, botnets are strategic: when network administrators try to block the attacks, botnets can shift to unprotected prey. Commercial cyber-security firms are trying to keep up with the changing threats; thus far, however, the botnets are staying at least one step ahead.

DDoS threats have been far more commercial than political. The driving force has been cyber-gangs (many of them based in the former Soviet Union and Southeast Asia) which are in the extortion business. They find a profitable Internet business that cannot afford downtime and threaten to take down its Web site(s) with DDoS attacks. The online gambling industry—by some estimates, a $15-billion-a-year business—is a particularly appealing target because it is illegal in the United States: it cannot seek protection and take advantage of robust U.S. communications infrastructure. Thus, administrators of popular gambling sites commonly receive threats of DDoS attacks and demands for $40,000-$60,000 to “protect” the sites from attacks during peak betting periods (say, before big sporting events such as the Super Bowl). Many legitimate businesses fall victim to cyber-extortion, too. Since it is better to dole out a little cash to stop future attacks than to deal with the PR fallout—and possible drop in stock prices—that usually follows cyber-attacks, cyber-crime is underreported and underprosecuted.

The risks to online freedom of expression may be considerable: saying anything controversial may trigger cyber-attacks that your adversaries can purchase easily.

Another commercial opportunity for cyber-gangs is the creation of a large army of for-hire botnets, with extremely powerful attack capabilities. It is currently quite straightforward to rent the destructive services of a botnet ($1000/day is a going rate). The point was made forcefully by a controversial recent experiment: a group of BBC reporters purchased the services of a botnet 22,000 infected-computers strong from a vendor of cyber-crime services and used it to attack the site of a cyber-security company.

The commercial availability of DDoS-attack capability has generated excitement about political applications. The risks to online freedom of expression may be considerable: saying anything controversial may trigger a wave of cyber-attacks that your adversaries can purchase easily. These attacks are financially burdensome and politically disabling for the victim. Getting your server back online is usually the least of your problems. Your Web hosting company may kick you off its servers because the cost of dealing with the damage caused by cyber-attacks usually outweighs the monetary gains of hosting controversial groups, from political bloggers to LGBT groups to exiled media from countries such as Burma (just to mention some recent victims of DDoS attacks). Protection from DDoS is available, but usually too expensive for nonprofits.

An alternative to expensive DDoS protection is a kind of distributed defense network. Imagine an idealized world in which every computer has the latest anti-virus update and where users do not open suspicious attachments or visit dubious Web sites. Cyber-gangs would then be left to their own devices—to attacking with computers they own—and the security issues would be considerably diminished. This perfect world is impossible to achieve, but the right policies could get us pretty close. One option is to go “macro”—to ensure that all critical national infrastructure is prioritized and protected, with extremely flexible resource allocation for the key assets (part of the job of a cyber-czar). This, however, would do little to curb the DDoS market. Indeed, it might embolden the attackers to ratchet up their capabilities. An alternative is to go “micro”—ensure that people who are responsible for the creation of this market in DDoS attacks in the first place (i.e., you and me) are knowledgeable (or at least literate) in cyber-security matters and do not surf with their antivirus protection turned off. This latter solution could eliminate the problem at root: if all computers were secure and computer users careful, botnets would significantly shrink in size. This, however, is a big “if,” and most skepticism over whether the federal government is well-placed to educate about these threats is justified.

The security threats from DDoS attacks pale in comparison with the *potential* consequences of another kind of online insecurity, one more likely to be associated with terrorists than criminals and potentially more consequential politically: data breaches or network security compromises (I say “potential” because very few analysts with access to intelligence information agree to speak on the record). After all, with DDoS, attackers simply slow down *everyone’s* access to data that are, in most cases, already public (some data are occasionally destroyed). With data breaches, in contrast, attackers can gain access to private and classified data, and with network security compromises, they might also obtain full control of high-value services like civil-aviation communication systems or nuclear reactors.

Data breaches and network security compromises also create far more exciting popular narratives: the media frenzy that followed the detection of China-based GhostNet—a large cyber-spying operation that spanned more than 1250 computers in 103 countries, many of them belonging to governments, militaries, and international organizations—is illustrative. Much like botnets, cyber-spying operations such as GhostNet rely on inadvertently downloaded trojans to obtain full control over the infected computer. In GhostNet's case, hackers even gained the ability to turn on computers' camera and audio-recording functions for the purposes of remote surveillance, though we have no evidence that attackers used this function.

In fact, what may be most remarkable about GhostNet is what did *not* happen. No computers belonging to the U.S. or U.K. governments—both deeply concerned about cyber-security—were affected; one NATO computer was affected, but had no classified information on it. It might be unnerving that the computers in the foreign ministries of Brunei, Barbados, and Bhutan were compromised, but the cyber-security standards and procedures of those countries probably are not at the global cutting edge. With some assistance on upgrades, they could be made much more secure.

In part, then, the solution to cyber-insecurity is simple: if you have a lot of classified information on a computer and do not want to become part of another GhostNet-like operation, do not connect it to the Internet. This is by far the safest way to preserve the integrity of your data. Of course, it may be impossible to keep your computer disconnected from *all* networks. And by connecting to virtually any network—no matter how secure—you relinquish sole control over your computer. In most cases, however, this is a tolerable risk: on average, you are better off connected, and you can guard certain portions of a network, while leaving others exposed. This is Network Security 101, and high-value networks are built by very smart IT experts. Moreover, most really sensitive networks are designed in ways that prevent third-party visitors—even if they manage somehow to penetrate the system—from doing much damage. For example, hackers who invade the email system of a nuclear reactor will not be able to blow up nuclear facilities with a mouse click. Data and security breaches vary in degree, but such subtlety is usually lost on decision-makers and journalists alike.

Hype aside, what we do know is that there are countless attacks on the government computers in virtually every major Western country, many of them for the purpose of espionage and intelligence gathering; data have been lost, compromised, and altered. The United States may have been affected the most: the State Department estimates that it has lost "terabytes" of data to cyber-attacks, while Pentagon press releases suggest that it is under virtually constant cyber-siege. Dangerous as they are, these are still disturbing incidents of data loss rather than seriously breached data or compromised networks. Breakthroughs in encryption techniques have also made data more secure than ever. As for the data loss, the best strategy is to follow some obvious rules: be careful, and avoid trafficking data in open spaces. (Don't put important data anywhere on the Internet, and don't leave laptops with classified information in hotel rooms.)

Gloomy scenarios and speculations about cyber-Armaggedon draw attention, even if they are relatively short on facts.

Although there is a continuous spectrum of attacks, running from classified memos to nuclear buttons, we have seen no evidence that access to the latter is very likely or even possible. Vigilance is vital, but exaggeration and blind acceptance of speculative assertions are not.

So why is there so much concern about "cyber-terrorism"? Answering a question with a question: who frames the debate? Much of the data are gathered by ultra-secretive government agencies—which need to justify their own existence—and cyber-security companies—which derive commercial benefits from popular anxiety. Journalists do not help. Gloomy scenarios and speculations about cyber-Armaggedon draw attention, even if they are relatively short on facts.

Politicians, too, deserve some blame, as they are usually quick to draw parallels between cyber-terrorism and conventional terrorism—often for geopolitical convenience—while glossing over the vast differences that make military metaphors inappropriate. In particular, cyber-terrorism is anonymous, decentralized, and even more detached than ordinary terrorism from physical locations. Cyber-terrorists do not need to hide in caves or failed states; "cyber-squads" typically reside in multiple geographic locations, which tend to be urban and well-connected to the global communications grid. Some might still argue that state sponsorship (or mere toleration) of cyber-terrorism could be treated as *casus belli*, but we are yet to see a significant instance of cyber-terrorists colluding with governments. All of this makes talk of large-scale retaliation impractical, if not irresponsible, but also understandable if one is trying to attract attention.

Much of the cyber-security problem, then, seems to be exaggerated: the economy is not about to be brought down, data and networks can be secured, and terrorists do not have the upper hand. But what about genuine cyber-warfare? The cyber-attacks on Estonia in April-May 2007 (triggered by squabbling between Tallinn and Moscow over the relocation of a Soviet-era monument) and the cyber-dimension of the August 2008 war between Russia and Georgia have reignited older debates about how cyber-attacks could be used by and against governments.

The Estonian case is notable for the duration of the attacks—the country was under "DDoS-terror" for almost a month, with much of its crucial national infrastructure (including online banking) temporarily unavailable. The local media and some Estonian politicians were quick to blame the attacks on Russia, but no conclusive evidence emerged to prove this. The Georgian case—widely discussed as the first major instance of cyber-attacks (primarily DDoS) accompanying conventional warfare—has barely lived up to its hype. Many Georgian government Web sites were, in fact, targets of severe DDoS attacks. So was at least one bank. Yet, the broader strategic importance of such attacks within the Russian military operation is not clear at all, nor did Russia acknowledge responsibility for the attacks.

Although the attacks on Estonia and Georgia are often grouped together—perhaps because of the tentative Russian involvement in both—they are also very different. One important difference is in the degree of technological sophistication of the two countries. Attacking the Internet in Estonia, which made Internet access a basic human right in 2000, is like attacking the banks in Lichtenstein: the country's economy, politics, and even some emergency services are pegged to it so tightly that being offline is a national calamity.

Georgia, on the other hand, is a technological laggard. When Georgia's major government Web sites became inaccessible during the war, the Foreign Ministry was slow in finding a temporary home on a blog. The lapse may have gone largely unnoticed: 2006 Internet statistics gathered by the United Nations show that Georgia had about seven Internet users per one hundred population compared to 55 in Estonia and 70 in the United States. The Georgian case also highlights the danger of drawing too many strategic lessons from cyber-attacks. After all, one common result of the loss of Internet access is power outages, common during wartime regardless of cyber-attacks.

Moreover, both Georgia and Estonia are in a sense "cyber-locked," with limited points of connection (even in Estonia) to the external Internet. This limited connectivity and the two country's dependence on physical infrastructure heighten their vulnerability. Less cyber-locked nations do not face the same risk. As Scott Pinzon, former Information Security Analyst with WatchGuard Technologies, told me, "If Georgia or Estonia were enmeshed into the Internet as thoroughly as, say, the State of California, the cyber-attacks against them would have been reduced to the level of nuisance." The smartest way to guard against future attacks may, then, be to build robust infrastructure—laying extra cables, creating more Internet exchange points (where Internet service providers share data), providing incentives for new Internet service providers, and attracting more players to sell connectivity in places that now have limited infrastructure. The United States has actually done quite a bit of this already, so the Estonian experience may have little to teach Americans. While it might benefit Estonia and some other countries to invest heavily in upgrades, the United States may be able to forego dramatic and costly changes in favor of regular maintenance and incremental improvements.

Quite apart from the technological issues of cyber-warfare, there is the question of what even constitutes cyber-war. How do existing legal categories apply in this new setting?

Using the metrics of conventional conflicts to assess these attacks is not easy. How severe must the damage be in order for the cyber-attacks to qualify as armed attacks?

For largely geopolitical reasons, Estonia initially called the cyber-attacks a cyber-war, a move that now seems ill-considered (on a recent trip to Estonia, I noticed that Estonian officials had replaced the term "cyber-war" with the more neutral "cyber-attacks"). The militarization of cyberspace that inevitably comes with any talk of war is disturbing, for there is no evidence yet to link the current generation of cyber-attacks to warfare, at least not in the legal sense of the term. However, the attacks on Estonia and Georgia did each pose an intriguing legal question, and neither has yet been answered definitively. First, do

cyber-attacks constitute a “use of armed force” as understood by international law (the Estonian case)? Second, what kind of cyber-attacks are allowed under the laws of war once the conflict has already begun (the Georgian case)?

The first question is the trickiest. Commenting on the attacks, the Estonian defense minister said “such sabotage cannot be treated as hooliganism, but has to be treated as an attack against the state.” But did the cyber-attacks constitute the beginning of an armed conflict, as understood by the Geneva Conventions or Article 51 of the United Nations Charter? If the cyber-attacks constituted an armed attack, Estonia’s NATO allies should have followed Article 5 of the North Atlantic Treaty, which treats an attack against one member state as an attack against all and calls for collective defense. NATO only sent a team of experts to assess the damage. Using the metrics of conventional conflicts to assess the severity of these attacks is not easy. How intense and severe must the damage be in order for the cyber-attacks to qualify as armed attacks? Does damage in cyberspace qualify, even in the absence of offline damage? Is inconvenience to Internet users enough? What about the duration of the attacks?

However such questions are answered, the aggrieved party would still have to prove that a cyber-attack was state-sponsored, and it is unclear how one makes this argument in a legally convincing fashion. Are states only responsible for actions they directly control? Are they also responsible for all cyber-activity in their territory? And how far does that responsibility extend? At least one computer with an IP address belonging to the Russian government was identified as part of a botnet used in the Estonian attacks, but it is hard to build a case for Russian government responsibility on that IP address alone, since there were thousands of other participating computers.

If state involvement cannot be proven beyond doubt, cyber-attacks should be treated as crimes and dealt with under national and, in some cases, international criminal law. But there are difficulties on this front as well. For example, unlike Estonia and many countries, Russia has never signed the Council of Europe Convention on Cybercrime, which is the first international treaty seeking to harmonize national laws and facilitate cross-border cooperation among states on issues of cyber-crime. This makes it impossible to hold Russia to the standards envisioned in the Convention, and international law also provides few mechanisms for punishment.

The second question—what kinds of attacks would be allowed under the law of armed conflict?—presents another theoretical challenge, though for now at least, existing legal standards may suffice to address the issues.

Common sense dictates that the severity and targets of such attacks should be guided by international law, particularly the Geneva Conventions and associated protocols. Broadly speaking, current norms state that the conduct of war must meet three fundamental standards: belligerents must *distinguish* military from civilian objects when selecting targets; *balance* military necessity with humanitarian concern (the choice of weapons is not unlimited and must be made with the avoidance of unnecessary suffering in mind); and shun the use of force that is *disproportionate*, in the sense that it shows insufficient

attention to the unnecessary suffering that might result. These principles have proved very hard, but not impossible, to interpret in conventional conflict; applying them to cyberspace is not an insurmountable challenge.

The careful application of these three principles to the conduct of war could explain why militaries might shy away from cyber-attacks. First, it is hard to predict the consequences of such attacks; cyber-attacks typically lack surgical precision and are notorious for side effects—a virus planted in a military network could easily spread to civilian computers, causing much unanticipated collateral damage.

Second, precisely targeted cyber-attacks could be a more humane way of conducting warfare. Instead of bombing a military train depot, with collateral civilian deaths, one can temporarily disable it by hacking into its dispatch system. However, the rules of war also stipulate that once a belligerent has used a more humane weapon, it ought to use that weapon in similar situations—and who would voluntarily abandon tanks in favor of computers only?

Third, most cyber-attacks are hard to justify in strategic terms and therefore would open associated personnel to prosecution for war crimes. For example, if there is little to be gained from attacking a poorly maintained Web site of the Georgian parliament, Russia could not justify an attack on it in military terms. If it went ahead with such an attack, its commanders woul risk prosecution for a disproportionate use of force.

The Internet does create one complexity worth considering in the context of applying existing laws of war: civilians on both sides can now participate in hostilities remotely. At the height of the war with Georgia, Russian blogs were full of detailed instructions on how to enlist in the cyber-war effort. Currently, humans are of little value in this process: a conventional botnet attack is more damaging. Yet, it is possible that human-powered botnets—or “meatbots”—could soon play a more serious role. Would participants then be liable for war crimes for their actions as civilians, who, unlike combatants, do not enjoy immunity under the law of war for their participation in hostilities? Would such civilian actions fall under the category of “direct participation in hostilities,” outlined in Commentary to Additional Protocol I to the Geneva Conventions (“Direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and the place where the activity takes place”)? We may need a special clarification of this concept for cyberspace, but other metrics—the damage caused, the targets chosen, and so forth—could still apply.

There is a line between causing inconvenience and causing human suffering, and cyber-attacks have not crossed it yet.

The legal options are also complicated in the case of classical rather than meatbot-powered DDoS attacks because there are often at least five parties to it: attackers, computer users whose machines are enlisted by the attackers, target Internet sites, software vendors responsible for the exploited security vulnerabilities, and various Internet service providers who deliver the attack traffic. These parties have different

degrees of responsibility, and some of them are liable for negligence, itself a murky legal area.

Putting these complexities aside and focusing just on states, it is important to bear in mind that the cyber-attacks on Estonia and especially Georgia did little damage, particularly when compared to the physical destruction caused by angry mobs in the former and troops in the latter. One argument about the Georgian case is that cyber-attacks played a strategic role by thwarting Georgia's ability to communicate with the rest of the world and present its case to the international community. This argument both overestimates the Georgian government's reliance on the Internet and underestimates how much international PR—particularly during wartime—is done by lobbyists and publicity firms based in Washington, Brussels, and London. There is, probably, an argument to be made about the vast psychological effects of cyber-attacks—particularly those that disrupt ordinary economic life. But there is a line between causing inconvenience and causing human suffering, and cyber-attacks have not crossed it yet.

The usefulness of cyber-attacks as a military tool is also contested. Some experts are justifiably skeptical about the arrival of a new age of cyber-war. Marcus J. Ranum, Chief Security Officer of Tenable Network Security, argues that it is pointless for superpowers to develop cyber-war capabilities to attack non-superpowers, as they can crush them in more conventional ways. As for non-superpowers, their use of cyber-capabilities would almost certainly result in what Ranum calls "the Blind Mike Tyson" effect: the superpower would retaliate with offline weaponry ("blind me, I nuke you"). If Ranum is right, we should forget about the prospect of all-out cyber-war until we have technologically advanced superpowers that are hostile to each other. Focusing on cyber-crime, cyber-terrorism, and cyber-espionage may help us address the more pertinent threats in a more rational manner.

In the meantime, those truly concerned about the future of the Internet, global security, and e-Katrinas would be advised to watch a recent *South Park* episode, in which the Internet suddenly disappears and hordes of obsessed families head to the Internet Refugee Camp in California, where they are allowed to browse their favorite Web sites for 40 seconds a day, while the military fights the no-longer-blinking giant Internet router. Finally, a nine-year-old boy plugs the router back in, and its magic green light returns. This would make a sensible strategy for many governments, which are all-too eager to adopt militaristic postures instead of focusing on making their own Internet infrastructures more robust.