Aux Armes, Citoyens: Cyber Security and Regulation in the United States

(pre-print version of article published in Elsevier's Telecommunications Policy, Fall 2005)

James Andrew Lewis
Center for Strategic and International Studies

1. Introduction

> For a quarter century, the nation -- and the world -- moved toward ever more reliance on markets, ever more confidence in business and ever less trust in government. But now the tide has turned.
>
> Editorial, *The Wall Street Journal*, 17 April 2002

Since the 1980s, deregulation and privatization have reduced the role of governments in economic affairs. After September 11, 2001, however, the United States government began to put in place new laws and regulations to strengthen homeland security. Security has become a central rationale for regulating commercial activities. However, one area continues to be relatively free from regulation. Despite ominous warnings of electronic "Pearl Harbors," the US has declined to intervene in the market or use regulation to improve cyber security. Instead it has depended on market forces and voluntary action to "engage and empower Americans to secure the portions of cyberspace that they own, operate [or] control…."(National Strategy to Secure Cyberspace, White House, p.VIII).

This makes cyber security[1] an anomaly. National defense and homeland security are public goods where individuals share in the benefits irrespective of how much they spend or if they spend at all. Markets are inefficient at supplying goods and services in situations where groups of people must work together to achieve a good outcome but the incentive for investment and cooperation is low. In these situations, the private sector will not produce an optimal outcome.

The requirements of homeland security have seen an expansion of regulation for immigration and transportation, law enforcement, banking, and communications, but US cyber security policy still assigns government a minimal role.[2] This is even more peculiar given the vivid warnings of the potential for catastrophic attack, "where," according to a 1995 Time Magazine Cover story, "a tyrant with inexpensive technology could unplug NASDAQ or terrorist hackers could disrupt an airport tower." (Time, 1995) Why eschew regulation if the risk is apparently so great? To explain this, we need to look at the background from which homeland defense and cyber security emerged.

2. New Threats

With the end of the Soviet Union, national security analysts in the US began to reassess

[1] Cyber security is the defense or protection of the integrity, operations and confidentiality of computers and computer networks.

[2] While some legislation, such as the Health Portability and Accountability Act of 1996 and the Graham-Leach-Bliley Financial Reform Act of 1999 have led to better network security, this has been a byproduct and not the intent of the laws.

the source and nature of post-cold war threats. As part of this reassessment, a series of influential studies in the 1990s focused policy makers' attention on "Homeland Defense" and the vulnerabilities of the information-communication technologies that were coming to dominate economic activity. The first such report was issued by the Joint Security Commission, established by the Secretary of Defense in June 1993, early in the Clinton administration. The Commission's 1994 report, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*, reviewed new threats to national security and discussed how the U.S should respond. The Commission called the security of information systems and networks "the major security challenge of this decade and possibly the next century" (JSC 1994, p. 1).

This was followed by a 1996 Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)*. In its executive summary, the Board advised that US national security increasingly relied on interdependent infrastructures that were vulnerable to cyber attack, and there was a need for "extraordinary action" to defend against information warfare.

A specially convened "National Defense Panel," created as part of the first congressionally-mandated Quadrennial Defense Review, examined US military priorities after the Cold War. The Panel's 1997 report to the Secretary of Defense concluded that asymmetric threats to the United States were increasing and becoming potentially more damaging. The panel recommended that the US pay greater attention to the defense of the American homeland. It emphasized that the US would need to prevent a range of attacks targeted at the American population and economic infrastructure, including cyber terrorism. [3]

These reports stress the increased risk of an opponent seeking asymmetric advantage, by attacking where a target is weak rather than where it is strong. An opponent gains asymmetric advantage by exploiting unexpected vulnerabilities or unconventional weapons. The reports identified the principle sources of asymmetric threats to US security as weapons of mass destruction and their proliferation, and threats to the American "homeland," its population and critical infrastructure. Information systems and the communications infrastructure were viewed as a special area of vulnerability.

The most influential report regarding cyber security appeared in October 1997. The Report of the Presidential Commission on Critical Infrastructure Protection, chaired by former General Robert Marsh, provided the basis for US efforts to protect critical infrastructure. The report did much to focus critical infrastructure protection on cyberspace. The Commission's report concluded: "The nation is so dependent on our infrastructures that we must view them through a national security lens" (PCCIP 1997, p. vii). The Commission predicted that the increasing reliance of the US upon critical infrastructures and cyber-based information systems would also create "a new dimension of vulnerability" (PCCIP 1997, p. ix). The Report made it clear that non-traditional attacks by a range of potential opponents on infrastructure and information systems could

[3] For another influential report see National Commission on Terrorism (2000).

significantly harm both the US economy and its military power.

3. New Style Governance

In response to the Marsh Report, the White House assembled a new bureaucracy for cyber security and began a process to develop a national strategy for securing cyberspace. Presidential Decision Directive 63 (PDD-63), signed in May of 1998, directed agencies to take necessary steps to ensure the continuity and viability of critical infrastructures.[4] It provided guidelines for addressing vulnerabilities, established a structure for infrastructure protection within the federal government, and called for a national strategy for critical infrastructure that highlighted cyber vulnerabilities. PDD-63 established a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism (a member of the White House staff) and two new agencies, the Critical Infrastructure Assurance Office (in the Department of Commerce) and the National Infrastructure Protection Center (in the Department of Justice), with responsibilities for cyber security. PDD-63 called for a "National Plan for Information Systems Protection" that focused federal efforts to protect critical cyber-based infrastructures, such as the electrical grid or the telecommunications network.

After this rapid start, it took almost three years to produce a national strategy. The long gestation period was due both to the extensive public consultations undertaken as part of the strategy's development and to the intense internal debates over the role of government. The debate pitted some national security officials, who favored energetic government intervention into cyberspace, against other parts of the Executive Branch (particularly the Office of Management and Budget and the Office of the President's Science Advisor) and the IT industry, who preferred self regulation and a voluntary approach.

After intense interagency battles, the Administration was able to issue *The National Strategy to Secure Cyberspace* in February of 2003. Early drafts of the strategy (widely circulated for private comment) had put forward specific recommendations for interventionist government policies (such as a greater federal role in ICANN or requirements for security features in browsers or operating systems,) but the final strategy did not contain these ideas. In fact, the *National Strategy* states that "federal regulation will not become a primary means of securing cyberspace" and that "the market will provide the major impetus" (White House 2003, p. 30). The strategy put forth a series of anodyne recommendations and homilies for best practices, and was perceived by many reviewers to be "toothless."[5] In pursuing the laudable goal of avoiding over-regulation, the strategy essentially abandoned cyber defense to an ad hoc reliance on market forces.

Several factors led to this unsatisfactory outcome. First, a larger trend of privatization and the long cycle of deregulation overlapped with the introduction of the commercial Internet. Telecom deregulation was a particularly important precedent as it included

[4] See White House (1998).

[5] For example, U.S. unveils cyber security plan. *BBC News*, February 15, 2003, at http://news.bbc.co.uk/2/hi/technology/2766029.stm. See also Diane (2002).

decisions to privatize services, break up national monopolies, simplify regulatory structures, and replace command-and-control mechanisms with a greater use of markets. It is not surprising that this should have carried over to the Internet in general and cyber security in particular. Since the economic infrastructure and the networks that comprise cyberspace were largely privately owned and controlled, government's role would be circumscribed, and the administration would not seek new authorities from legislation or regulation.

As the US government commercialized the Internet in the mid-1990s, it adopted an explicitly "hands-off" approach to Internet governance that sought to shift responsibility and control to the private sector. The first Clinton administration eCommerce "czar," Ira Magaziner (1998), said, "The first principle is that this will be an environment or a world where private actors lead, not governments." This principle shaped Internet policy, most notably in the decision to privatize management of the domain name system by turning it over to a private corporation, ICANN. The emphasis in the Executive Branch on privatization and deregulation was reinforced by the belief that "the digital economy moves too quickly and requires too much flexibility for the processes of government to be, in most cases, successful in relating to it" (Magaziner 1998).

The second factor was the business community's strong desire to avoid any new government mandates. One leading industry association, Business Software Alliance, called for the federal government to limit its efforts to leading by example and stated that "industry, through the marketplace, can lead the way" to better Internet security.[6] After reviewing ***The National Strategy to Secure Cyberspace***, the Information Technology Association of America was "gratified that . . . the Administration has issued a plan that recognizes the need for partnership and participation to protect cyberspace -- not mandates and government intervention."[7] A third noted that "regulatory processes are too slow and cumbersome to keep technology growing at top speed" while the Electronic Industry Alliance states:"Current policies and laws related to cyberspace are also likely to add to the barriers [to internet security] because they are drastically behind the pace of technology."[8] Business statements on cyber security emphasized the benefits of public-private partnerships, voluntary action, and information sharing.[9]

The experience of the struggles over the Communications Access for Law Enforcement Act and the encryption wars, where the federal government had attempted to mandate the use of the "clipper chip" or key escrow, reinforced the belief that for e-commerce and for security, market forces and the private sector should shape cyberspace. The primary intent of encryption regulation was to ensure continued government access to communication. However, the Departments of Defense and Justice and the FBI also wanted to see the widespread implementation of this regulation in order to build "secure

[6] See comments at http://www.bsa.org/eupolicy/Industry.cfm
[7] See comments at http://www.itaa.org/isec/pubs/e20032-05.pdf
[8] See comments at http://www.eia.org/new_policy/internetsecurity.phtml
[9] In addition to notes 6, 7, and 8, see "The Business Roundtable Welcomes Announcement of The National Strategy to Secure Cyberspace," Press Release, 09/18/2002; U.S. Chamber of Commerce, "Regulatory Issues."

public networks (White House 1996). The harsh reaction of the private sector to clipper and key escrow strengthened the desire for a voluntary, market-based approach to cyber security.

The third factor was Y2K. Preparations for potential software problems that might occur with the advent of a new millennium (also known as Y2K bug) had a profound affect on cyber security. In retrospect, it appears that the Y2K crisis was somewhat exaggerated, but at the time many saw it as a useful model for partnership between government and the private sector in responding to network vulnerabilities. Y2K did seem to hold the promise of a new kind of approach to public problems, one where a cooperative, informal and voluntary relationship between government and the private sector replaced command-and-control regulations. Among those citing Y2K as a model, Comptroller General David Walker noted in Congressional testimony that "government can learn from the strategies devised to deal with the Year 2000 problem," while ITAA President Harris Miller called for a global response to information and cybercrime problems modeled on Y2K.

However, the Y2K response had two parts. The first was a government effort to educate, to cooperatively develop responses, and to lead by example. This became the template for a voluntary approach for cyber security. The second was a government mandate, through Securities and Exchange Commission (SEC) regulations, for publicly traded companies to report on the steps they had taken to secure their networks and their operations from disruption. In retrospect, this SEC requirement may have been at least as important as anything else in getting companies to put safeguards in place. Y2K was a new model for government intervention, but the key to its success was that this model blended voluntary action and regulation.

In fairness, a globally distributed collection of nonhierarchical networks does not fit easily with regulation by national governments. Additionally, no single agency could claim jurisdiction over the cyber security problem. The very newness of the Internet and the hyperbole that accompanied its early days also made analysis and planning difficult. These factors deterred governments from seeking an active role in internet governance or security.

4. Reassessing the Cost of Regulation

In retrospect, the policy process of the 1990s assigned too much responsibility for cyber security to the private sector for functions it could not easily perform. This was the result in part of an estimate of the potential cyber threat that saw it as protean and immense, and addressable only by some large-scale collective effort. A first step in reassessing these policies is to examine the fundamental assumption underlying the new thinking on security and infrastructure vulnerability. That assumption is that nations and critical infrastructure have become dependent on computer networks for their operation, creating new vulnerabilities that a hostile nation or group could exploit and that an attack that disabled these networks would cause terror or deal crippling blows.

The reports noted above identified a new area of vulnerability for the US. Policy

development proceeded from a broad but untested assumption of national vulnerability to cyber attack. This assumption, in combination with a predisposition against broad regulation, led the US government to adopt a voluntary and inadequate approach to cyber security. None of the reports identified where the risks from cyber attack were greatest and, therefore, where risk to the public interest and the State sufficient to overcome the rights of private ownership.

Catastrophic cyber attack scenarios worked against government intervention, as they seem to require for broad and intrusive regulatory authorities in response. Broad new regulations would be difficult to design, implement and manage and could easily have an undesirable economic effect.

If, however, regulation were required only in targeted, select circumstances, their imposition would not face so daunting a set of obstacles. Painting a broad picture of potentially grave threats to the entire economy raised the cost of regulation and made government intervention appear prohibitively expensive. A more accurate assessment of the threat would make the option of regulation more attractive and more manageable, as a limited government intervention would be sufficient to improve security.

The assumption of broad vulnerability that guided PDD-63 and the *National Strategy* can be criticized in several areas: the vulnerability of infrastructure, the effect of cyber attacks on society, and the probability of terrorist use of cyber weapons. An examination of critical infrastructures and reported incidents suggests that while computer networks are vulnerable to attack, critical infrastructures are not equally vulnerable. Computer networks do not yet play the pervasive and dominant role assumed in cyber-terror scenarios, terrorists are attracted to more violent methods of attack than is offered by cyber weapons, and industrial societies, with their redundancy of services and equipment and their ability to quickly repair and restore, are robust and resilient in the face of attack.

4.1. Utilities

The very diversity of infrastructure in the US, with thousands of public and private entities providing service, makes a "Pearl Harbor" unlikely. They use diverse network technologies and systems architectures. This complicates the terrorists' task. The American Waterworks Association's assessment of the terrorist threat to water supplies placed "physical destruction of the system's components to disrupt the supply of water" as the most likely source of infrastructure attack (DeNileon, 2001; see also Berinato, 2002). Electrical utilities are subject to thousands of hacking incidents every year, but these attacks have not disrupted service (Riptech Inc., 2002). The failure of the Northeast electrical grid in August 2003, while embarrassing, did not create panic or damage national security. The Information Assurance Task Force of the National Security Telecommunications Advisory Committee concluded "Physical destruction is still the greatest threat facing the electric power infrastructure. Compared to this, electronic intrusion represents an emerging, but still relatively minor, threat."[10]

[10] See Information Assurance Task Force of the National Security Telecommunications Advisory Committee, at http://www.aci.net/kalliste/electric.htm

Fixed line telecommunications networks remain particularly robust, in part because of a legacy of defense preparations that date back to the 1950s. Working in partnership with Federal agencies, telecommunications companies took steps to build in redundancy and survivability and to enhance physical and network security. This makes some contribution to Internet reliability. Although the Internet was designed to survive nuclear war, it may have points of failure that could be exploited to create system-wide disruption, such as potential vulnerabilities in the domain name system and routing protocols. However, this would be unlikely to result in terror. Individuals would turn to alternate means of communications. Most industrial countries now have access to three or four different modes of communications, such as wireless and satellite links, providing redundancy and making communications more robust than a decade ago.

4.2. Public Safety

Cyber disruption of 911 systems is also unlikely as there are thousands of local "911" systems using different technologies and procedures. Hacking has disrupted no emergency response function in a major city. Some press reports said that the "Slammer" virus damaged 911 systems (Vamosi, 2003). Slammer's effect was to slow the database program dispatchers used to log calls. Faced with the slowdown, dispatchers used paper and pencil logs until computer service was restored. Response time by emergency services was not affected, and there was no degradation of 911 services (Wells, 2003). It might be possible to spam email addresses with messages instructing people to call 911 for important information and thus overload the system (this tactic was used in the 1997 US exercise "Eligible Receiver"), but this trick usually works only once. However, in conjunction with a bombing or other physical attack, this practice could act as a "force multiplier" for a terrorist event, and improvements in anti-spam software limit the effectiveness of this tactic.

4.3. Transportation

The transportation infrastructure in the US is even less vulnerable to cyber attack. Most cargo travels by ship, truck or rail. Within the US, trucks and the national highway system would be difficult targets for cyber attack. A disruption of rail service would see cargo shift to other railroad companies or to long-haul trucks. Similarly, the risk to safety of flight is overstated (Paul, 2001).[11] Computer networks do not operate aircraft. Neither Eurocontrol nor the Federal Aviation Authority depends on computer networks or the Internet to manage air traffic. The air traffic system is used to routine delays and disruption and experienced in responding to them to keep flights moving. The high level of human involvement in flight operations and air traffic control makes cyber attacks improbable.

4.4. Finance

[11] Paul notes: "Examples of cyber terrorist actions can include hacking into an air traffic control system that results in planes colliding…"

The financial sector has taken extensive measures to secure its networks, both in response to regulation and as an extension of their normal concerns for security, including the use of authentication**,** encryption, firewalls, intrusion detection and reviews by the Federal Reserve. Network security varies among individual banks, but crippling a bank's network is more likely to cause inconvenience rather than terror. There is some concern that there could be a single point of vulnerability, such as Fedwire (the U.S. government network responsible for money transfers) that could affect the financial sector broadly. The experience of September 11, 2001, where physical attack badly damaged the major trading financial center in the US and affected Fedwire showed the extent of the damage that an attack on the financial system could create (expensive, but not catastrophic) and motivated investment and financial institutions to improve security. A study by Dartmouth's Institute for Security Technology Studies (2003) concluded, however, that the financial system is more at risk from physical attacks (against physical or cyber structures) than cyber strikes.

4.5. Manufacturing

Economic activity is increasingly dependent on information technology. However, economic warfare in the form of a cyber attack is unlikely to damage production to the point where it affects security (Bradsher, 2000). First, cyber attack would not produce the physical damage and disruption of high explosives. This means that recovery from an attack will be much simpler. Cyber weapons are intrinsically less effective than blast. We know from a number of surveys that industrial societies are impressively resilient and that even sustained air attack with conventional munitions will not cripple or defeat an opponent.[12] With a global supply chain and multiple suppliers for most goods and services, shutting down a factory or company would go unnoticed. Affected companies would experience losses; competitors might experience increased profits. Some companies now report that because of defensive measures they have taken, viruses that were exceptionally damaging when they first appeared are now only "nuisances" (Riptech Inc., 2002).

Cyber attacks have not shut down any critical infrastructures nor have they created terror. In a decade of major terrorist activity directed against the US, there have been no cyber attacks that damaged US infrastructure, affected US military operations, led to casualties or created panic. Computer network failures do not result in catastrophe or terror. While terrorists have exploited vulnerabilities in civil society and use commercial technologies to create shock and horror, none of their attacks has used cyber weapons, perhaps because cyber attacks do not provide the effect that terrorists seek. Most accounts of risks associated with cyber attacks underestimate the ability of nations to resist and to respond rapidly to attack. Not only are modern societies more resilient, with their large pool of talent and resources, than the cyber terror school gives them credit for, but the response of nations to an attack is often stiffer resistance, not collapse.

[12] The most detailed of these is the U.S. Strategic Bombing Survey, Summary Report (European War), 1945. http://www.anesi.com/ussbs02.htm

An assumption of massive cyber vulnerabilities that were deeply embedded across the entire economy fails to take into account the diversity of economic actors and activity. A more realistic picture that identified the small number of key infrastructure facilities that might be at risk form cyber attack – could have clarified the scope and role of government action and made the problem more manageable. In doing so, it could have helped place an interventionist role for government in cyber security into the larger and beneficial deregulatory trend that emphasizes smaller role for government agencies, less regulation, decentralization and more reliance on markets. The record of cyber attack, or rather the record of its absence, suggests that the risk is manageable and therefore that cost of regulation to the broader economy could be low.

5. New Model Regulation

Defense and security are public goods. The market will not supply them in sufficient quantity to meet a society's needs. A reliance on voluntary action and proselytizing the adoption of best practices guarantees inadequate security. The difficulty, in an era of broad economic deregulation and intrusive homeland security regulation, is to find an approach that preserves as much as possible of the economic benefits of minimal government interference in the economy while not sacrificing the public interest in greater security on the altar of deregulation.

The current voluntary approach is inadequate to provide for the public good. Relying on voluntary efforts to produce a public good always results in a shortfall. Economic pressures work against voluntary action. An increasingly competitive market provides companies with the incentive to become more efficient. Eliminating redundancy and investing capital in functions that provide the best return are in the long term economic and security interests of the US. Firms will devote resources to cyber security, but this will not be enough for homeland security. This "public good gap" is the difference between the amount that the market will lead the private sector to spend on cyber security and the optimal amount for national security (NAERC, 2002; Hilt, 2003). In these situations, the private sector will not produce an optimal outcome. This shortfall in investment means that there has been "market failure" when it comes to cyber security.

The traditional response to market failure is government intervention. Cyber security poses a "collective action" problem (like national defense, automobile safety or environmental protection) that is best addressed by a governmental solution in the form of mandatory requirements. Where then would regulation be appropriate, and what level of regulation is required to provide security? In a perfect market, the private sector would purchase adequate security and firms would offer the products needed for it. This has not been the case. While some industry sectors (such as financial services) have moved to increase security, other sectors may not improve absent further incentives. Despite arguments that market forces and the evolution of the IT industry will improve security voluntarily, we must ask if cyber security, as with health, environmental, or safety issues, requires government intervention.

Better cyber security will require abandoning "electronic Pearl Harbor" scenarios and making an effort to identify critical and vulnerable infrastructures where some form of federal regulation or oversight is justified from the great majority of economic enterprises. Predictions of overwhelming catastrophe, actually limit the ability to develop a focused, defined response that could prove effective in improving security. Better cyber security would also require subsuming cyber security into a larger critical infrastructure protection strategy, in recognition of the secondary role cyber attack plays in potential attack scenarios. A failure to make this effort means a dilution of effort and inadequate security for key infrastructures.

A serious cyber defense would map individual infrastructure systems and networks, assess the vulnerability of different equipment and configurations, and then rank the utility in order of importance in the national infrastructure. Utilities that support large urban areas and collocate with military facilities or important industrial plants could be more important that utilities in, say rural areas. These key facilities could be "hardened" by adding redundancy, contingency plans, ensuring the existence of non-networked controls, and adding additional monitoring of functions.

This does not mean that all industries and infrastructures must be regulated or held to higher security standards. Not all infrastructure and networks are critical. A more focused set of regulations that would apply to a few crucial networks directly involved in key infrastructures for major urban areas – electricity, telecommunications, transportation, government services and perhaps a few others – deserve special attention. The damage to national security and public safety that could result from a successful attack on these few infrastructures justifies regulation. For the rest of the economy, interruption of computer networks poses no real risk to security. In this case, cyber security can be defined as a law enforcement and business problem best left to the private sector.

Voluntary action coordinated and informed by government is not sufficient for homeland security. Federal regulation is necessary for real progress. Law and regulation are incentives to encourage certain behaviors. Legislation and regulations (or even the threat of legislation and regulations) will energize the private sector to move faster in cyber security. Regulation can avoid a heavy-handed, prescriptive approach and instead aim to increase transparency and assign responsibility, leaving it up to individuals as to how best to meet requirements. The US has already imposed regulation on cyber security through the vehicle of legislation designed for other purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Financial Reform Act (GLB), and the Public Company Accounting and Investor Protection Act of 2002 (known as the Sarbanes Oxley Act), by creating responsibility for privacy (and consequently security), worked to increase awareness and demand for security products are useful examples of this.

HIPAA required the Department of Health and Human Services (HHS) to develop standards and regulations for transmission and storage of health information that identifies individual patients. The intent of HIPAA was to protect privacy, but it also affects security procedures. HHS developed a security standard with input from

standards groups and industry that is technology-neutral and scaleable. Health organizations that transmit or store electronic health information must conduct a risk assessment and develop a security plan to protect this information. They must document these measures, keep them current, and train their employees on security procedures. The security standard is divided into four categories: administrative procedures, physical safeguards, technical data security services, and technical security mechanisms to prevent unauthorized access to data transmitted over a communications network.

Section 504 (a) of GLB established a federal standard for financial privacy. As part of GLB, federal and state regulators were required to establish comprehensive standards for ensuring the security and confidentiality of consumers' personal information. The privacy provisions apply to any company engaged in financial services, whether affiliated with a bank or not. GLB covers finance companies, insurance companies, securities dealers, and even travel agencies. The Federal Trade Commission published regulations implementing GLB that went into effect in May 2000 (Federal Register, 2000).

Sarbanes-Oxley promises to have the most far reaching effects, as it applies to all publicly traded companies and will affect accounting standards that apply to companies that are not traded. Sarbanes-Oxley requires the Chief Executive Officer and the Chief financial Officer of a company to sign an annual statement attesting to the accuracy of their financial reporting and that they have exercised “due diligence” in ensuring this accuracy. Part of this due diligence is found in Section 404, which requires organizations “to establish and maintain an adequate internal control structure and to assess the effectiveness on an annual basis.” This includes control objectives for information technologies and networks and their security. The unintended consequence is that senior corporate officials are now required to attest that they have made efforts to secure their information systems.

While these regulations will force better cyber security, the problem with them is that none were designed to improve homeland security and they may not fully meet all homeland security needs. An effective homeland security strategy would identify the relatively small number of key networks and, impose higher standards of network security on them. The mechanism for developing these standards does not need to be old-style command and control regulation. An emerging alternative is to blend industry-developed standards and self-certification with federal enforcement of these standards. This avoids problems found with prescriptive regulations and with a purely voluntary approach. Government agencies can be slow in developing technically proficient standards. Private sector groups are weak on enforcing voluntary standards. This more complex regulatory model moves beyond a purely voluntary approach to reinforce cyber security with mandatory action while avoiding the overregulation that initial efforts sought to avoid.

6. Conclusion

Militias are the kind of military adopted by nations that lack the resources for a professional army. The national strategy for cyber security resembles a militia. All

citizens are to seize whatever lies close to hand and rush off to repel the invader. This approach generally has not worked, for the same sorts of reasons that afflict the national cyber security strategy – the population is ill equipped and trained and shows a lack of interest, and private firms are unwilling to invest in a public good. The U.S. model for cyber security should not be based on a verse from the "Marseilles" calling citizens to arms.

Federal initiatives for homeland security have profound implications for how the government will interact with the economy. Efforts to protect security undertaken by the U.S. (and now being considered by many other countries) have become a check on the larger the tide of deregulation. The experience of the National Strategy shows that these efforts will need to engage in a more complex interaction with private sector actors than was the case in the past. The mix of security concerns, deregulation and privatization has led to a new kind of public policy, where governments share responsibility for some functions with the private sector and seek to manage this responsibility through public/private partnerships.

Adam Smith wrote that there are some functions that the market will not necessarily provide, or provide well. He used the example of highways and mental institutions as activities where the market would not adequately provide for society's needs. Security on the internet, which combines aspects of both, is one such activity. While governments were initially leery of regulating the Internet, we have entered a period in which governments actively intervene in Internet governance and where the Internet is moving to a more regulated environment. The unavoidable problem of determining where and how to regulate for cyber security will grow more complicated as the US moves ahead with a major reorientation of its security policies.

References

Berinato, S. (2002). Debunking the threat to water utilities. *CIO Magazine*, March 15, at http://www.cio.com/archive/031502/truth_sidebar2.html

Bradsher, K. (2000). With its e-mail infected, Ford scrambled and caught up. *The New York Times*, May 8, p. C1.

Defense Science Board (1996). *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)*, at http://cryptome.org/iwd.htm

DeNileon, G. (2001). The who, what, why and how of counter-terrorism issues. *American Water Works Association Journal*, 93(5), 78–85.

Diane, F. (2002). Cyber security plan on the lite side. *Federal Computer Week*, September 23, at http://www.fcw.com/fcw/articles/2002/0923/news-cyber-09-23-02.asp

Federal Trade Commission, Privacy of Consumer Financial Information: Final Rule, Federal Register, Vol. 65, No. 101, May 24 , 2000

Hilt, D.W. (2003). *North American Reliability Council: Compliance Program*, February 4, at http://www.ferc.gov/industries/electric/indus-act/smd/conf-2003/02-04-03-nerc.pdf

Institute for Technology Studies (2003). *Survey and Analysis of Security Issues in the U.S. Banking and Finance Sector*, at http://www.ists.dartmouth.edu/ISTS/ists_docs/secfin0903.htm

JSC (Joint Security Commission) (1994). *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence*, at http://www.fas.org/sgp/library/jsc/

Lewis, J. A. (2003). Cyber terror: Missing in action. *Knowledge, Technology and Policy*, 16(2)

Lewis, J. A. (2002). Assessing *the Risks of Cyber Terrorism, Cyber War and other Cyber Threats*, at http://www.csis.org/tech/0211_lewis.pdf
Magaziner, I. (1998). Democracy and Cyberspace: First Principles. Keynote address, MIT's conference on Democracy and Digital Media, May 8, at http://web.mit.edu/m-i-t/articles/index_4_m1.html
Miller, Harris, "Developing Public-Private Partnerships to Strengthen Global Information Security in a Borderless World," Information Technology Association of America, May 30, 2002 http://www.itaa.org/infosec/RSAJapan5-30-02.pdf
National Commission on Terrorism (2000). *Countering the Changing Threat of International Terrorism*, at http://www.fas.org/irp/threat/commission.html
NAERC (North American Electric Reliability Council) (2002). Comments of the North American Electric Reliability Council to the Federal Energy Regulatory Commission on the Notice of Proposed Rulemaking for Standard Market Design," December 6.
National Defense Panel (1997). *Transforming Defense: National Security in the 21st Century: Report of the National Defense Panel*, at http://www.fas.org/man/docs/ndp/toc.htm
Paul, L. (2001). When cyber hacktivism meets cyberterrorism. *SANS Institute White Paper*, February 19, at http://www.lib.iup.edu/comscisec/SANSpapers/paul.htm
PCCIP (President's Commission on Critical Infrastructure Protection) (1997). *Critical Foundations: Protecting America's Critical Infrastructure*, at http://www.timeusa.com/CIAO/resource/pccip/intro.pdf
Riptech Inc. (2002). *Riptech Internet Security Threat Report*, July, at http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf
Vamosi, Robert, "How the Feds Failed Us When Slammer Attacked," ZDNet, February 3, 2003, http://reviews-zdnet.com.com/4520-7297_16-4207842.html
Waller, Douglas, "Onward Cyber Soldiers," Time Magazine, August 21, 1995, Volume 146, No. 8
Walker, David, Testimony before the Senate Government Affairs Committee, September 21, 2001, General Accounting Office
Wells, R. M. (2003). Dispatchers go low-tech as bug bites computers. *Seattle Times*, January 27, p. B1.
White House (2003). *The National Strategy to Secure Cyberspace*, at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
White House (1998). *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, at http://www.usdoj.gov/criminal/cybercrime/white_pr.htm
White House (1996). *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, at http://www.epic.org/crypto/key_escrow/white_paper.html
The Global Information Infrastructure, May 17, at www.epic.org/crypto/key_escrow/white_paper.html