Foreword

Michael Chertoff*

I am proud to be asked by the *Journal of National Security Law & Policy* to introduce this important and impressive issue. The timing could not be more critical. The nation is in the middle of a significant debate – how important is cybersecurity among the many security vulnerabilities competing for scarce resources? This is precisely the sort of consequential topic regularly addressed by this journal, which was created on a volunteer basis as a direct reaction to the September 11 attacks on the United States. My compliments to the *Journal* for providing incisive commentary by and for public officials and academics alike.

A cornerstone of our twenty-first century economy is the ability to employ computers to transact business, operate infrastructure, and manage our personal affairs. We often take for granted how much of our daily lives depends upon the efficient operation of our computers and their ability to communicate across vast and varied networks. Not just mobile phones, email, and online shopping rely on cyberspace, but also electricity and the businesses that facilitate our daily living like grocery stores and trash pickup. This dependence on cyberspace means that it must be reliable and resilient – in other words, secure from failure, compromise, data manipulation, or theft.

Of course, cybersecurity is only one aspect of national and homeland security. We are fighting against Taliban insurgents in Afghanistan, hardening the transportation system, and investing unprecedented resources in securing our national border. We undertook a massive immunization effort across our country's school systems to address H1N1 influenza. How do we assign a relative value to cybersecurity among this list of priorities? And once we determine the relative values, how do we take action to secure cyberspace? These matters are just beginning to be opened to robust debate. And that debate must take place within a common framework of analysis.

The answer to the first question is straightforward, if surprising. Cybersecurity is among our first rank of security priorities in the twenty-first century. The probability of cyber attacks is 100 percent – we continue to suffer regular, ongoing, damaging intrusions by nations committing espionage, criminals stealing data, and hackers seeking to damage computer systems. The potential consequences are high. Network electronic warfare can cripple or paralyze domestic and civilian systems; we have seen examples of this over the past few years in attacks aimed at Estonia and

---

* Former Secretary of the Department of Homeland Security (2005-2009). Since April 2009, he has served as the founding Principal of the Chertoff Group. The author thanks Gary M. Shiffman for research and editorial assistance and Larry Castro for comments on earlier drafts.

Georgia. At the same time, spies have exfiltrated sensitive security and communications data from our networks, and criminals have pilfered millions of dollars' worth of sensitive personal financial information.

The harder question is: How do we secure this cyberspace? To some, the idea of cybersecurity may seem at odds with the open architecture of the Internet, and with the spirit of freewheeling innovation that some Internet advocates cultivate. But no human activity can be fully productive without boundaries and rules – the full benefits of the automobile can only be realized with roads marked by lanes, directional signs, and traffic lights.

Our reliance on cyberspace without adequate cybersecurity presents a potential tragedy of the commons scenario unfolding before us. In the traditional telling of the story, the "commons" is a valuable resource like land on the village common that gets destroyed by individual ranchers acting in their own self-interest by overgrazing the grass. Suboptimal outcomes ensue without fencing or the adoption of enforceable standards to govern each rancher's behavior. Like the village common, nobody owns cyberspace. To secure this valuable resource, we will witness the creation of fencing – perhaps in the form of private clouds – and the adoption of enforceable standards.

What is the role and responsibility of government in securing the Internet? In the realm of physical security, government at all levels often plays the critical role, either by enforcing the law, guarding public physical facilities, or responding to emergencies. The private sector participates by protecting its own privately owned facilities or domains. Generally, private security efforts are subordinate or supplementary to government authority.

But cybersecurity presents a special case. We cannot simply assume that the federal government will or should bear exclusive or even predominant responsibility for solving the security problems associated with the Internet. Because much of the cyber world involves communication, engagement by government in securing that world potentially impinges on freedom of communication. This has First Amendment as well as other civil liberties implications. Thus, demarking the relative roles of government and the private sector in cybersecurity requires a special sensitivity to the degree of government control we want to allow over the Internet.

Determining the respective roles of government and the private sector is important. That allocation will determine the priorities and drive investment in capabilities. For cybersecurity, at the broadest level, we can think of responsibility allocated to governmental, commercial, public non-commercial (such as schools or nongovernmental organizations), and individual actors. Within those areas of cyberspace requiring high-level federal action, we have three sources of legal and practical authority: military action under Title 10, intelligence activities under Title 50, and criminal and civil legal powers under Title 18 and Title 28.[1]

1. As the Secretary of the Department of Homeland Security, I played a role in developing the framework for the federal government, working across the challenges of

With this in mind, a cyber risk must be addressed like any other risk to public safety and national security. As Secretary of the Department of Homeland Security (DHS), I advocated a risk-based approach to security.[2] I suggest the same approach to those thinking about securing cyberspace. People cannot be protected against all threats at all times. In the risk-based approach we used at the DHS, decision makers evaluate risk (R) as a function of threats (T), vulnerabilities (V), and consequences (C).

$$R = f(T, V, C)$$

Of course, the benefits of security come with associated costs.[3] Evaluating the optimal balance between costs and benefits is a threshold requirement. This balancing requires consideration of intangible as well as quantifiable values. Any assessment of security costs and benefits will consider the financial effects in both categories. But non-monetary costs such as diminution of civil liberties are also relevant. So too are psychic benefits of increased security, such as greater protection for privacy and greater confidence in cyberspace as a medium for personal as well as business communication. Finally, once we have calculated risk and considered cost/benefit tradeoffs, we must assign responsibility across the relevant institutions – governmental (military, intelligence, and civil), commercial, and public noncommercial.

Within the sphere of the federal government, the Secretary of the DHS serves as the principal federal official responsible for coordinating federal government efforts to secure the homeland, including cyberspace. Coordinating the security of the homeland can mean assuring that a specific department or agency of the government has accepted responsibility for, and taken steps to secure, its sector of the nation's critical infrastructure. It also requires facilitating information sharing about threats, and managing operational responses across government agencies. The federal cyberspace includes the top-level "mil" domain, where the Department of Defense (DoD) takes responsibility and possesses the greatest means. For other top-level domains – "gov," "edu," "com," "org," and "net" – the DoD does not possess the authority for security. The "gov" domain encompasses the boundaries of numerous government agencies, and the other domains are the responsibility of multiple commercial providers and users.

---

military, intelligence, and civil authorities. *See generally* MICHAEL CHERTOFF, HOMELAND SECURITY: ASSESSING THE FIRST FIVE YEARS (2009).

2. *See id.*; DEPARTMENT OF HOMELAND SECURITY, NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION AND RESILIENCY (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (providing a full explanation of the risk-based approach); *see also* John Garrick, *Perspectives on the Use of Risk Assessment To Address Terrorism*, 22.3 RISK ANALYSIS 421 (2002).

3. *See, e.g.*, Gary Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

The DoD has the statutory mission to secure the "mil" domain and significant capabilities to do so. The DoD has recently decided to establish the U.S. Cyber Command, making a significant organizational advance in how the DoD is organized to conduct computer network operations, both defensively and offensively. In particular, the merger of cyber defense and intelligence envisioned in the Cyber Command construct allows for a more robust cybersecurity capability based in part on intelligence-driven network situational awareness.

The "gov" domain is more difficult. Many agencies of the U.S. government participate in and rely upon the "gov" domain. After some amount of debate, the DHS has the lead to coordinate securing the "gov" domain, with both OMB and the White House Cybersecurity Coordinator remaining significant players. This is consistent with Homeland Security Presidential Directive (HSPD) 5, which provides that:

> (4) The Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.[4]

In practice, the DHS's primary initiative over the last year has been the Trusted Internet Connection (TIC) effort, which seeks to reduce the number of points at which "gov" users can enter the Internet. This initiative complements the intrusion detection capabilities of the National Cyber Protection System (NCPS), also known as "Einstein." The DHS is deploying an "Einstein 2" intrusion detection capability at an increasing number of federal departments and agencies, and anticipates deployment of an upgraded sensor capability, "Einstein 3," at a reduced number of Internet connections.

---

4. Homeland Security Presidential Directive5, (Feb. 28, 2003), *available at* http://www.fas.org/irp/offdocs/nspd/hspd-5.html.

To realize its responsibility to coordinate cybersecurity across the government, the DHS must have commensurate capabilities. Beyond the TIC and Einstein initiatives, the Department includes the U.S. Computer Emergency Readiness Team (U.S. CERT), which leads the federal civil efforts at response and risk management.[5] But this may not be enough in the medium-to-long term. To leverage all elements of federal power, the DHS must develop ways to employ the DoD's and the Intelligence Community's significant capabilities under the DHS's civilian auspices. This can be achieved through DHS authorities.

The most difficult of the domains to address are the nongovernmental ones ("com," "edu," "net," and "org"). Some suggest that the federal government should directly manage the security solution, just as in the "gov" domain.[6] Others oppose a robust government role and provide charged but entertaining videos on the Internet to make their points.[7] Although it is undeniable that the Internet can flourish only if it is safe and secure, we must proceed with caution when defining the government's role in managing private sector domains.

Some tentative thoughts: We must be careful not to allow the government to infringe unduly upon private freedom in an area so central to free speech and other freedoms. In my view, this means that the government should not have its hands directly on the levers of power over the Internet. There is more danger if the government directly operates civilian domain security, as opposed to simply setting standards for security and enabling private entities to operate the security function in private space. Perhaps the best solution is to create or authorize trusted private third parties that can receive intelligence and capabilities from the government – information such as classified threat reporting and the latest malicious software signatures. These organizations would then distribute the information and capabilities to the private sector and even go so far as to operate network defense. These third parties – a type of "cyber escrow agent" – could ensure that the benefit of government expertise is available to the private sector, but act as a check and balance to prevent the government from exerting direct control over the domain. Under this approach, if there were to be an instance of government overreach, the trusted third party would be empowered to go to court to prevent inappropriate government actions.

For the DoD, securing the "mil" domain needs to be a part of strategic

---

5. The venerable Posse Comitatus Act embodies the traditional desire to limit direct military involvement in the domestic civilian arena. *See* 18 U.S.C. §1385 (2006) (using the Army and Air Force as *posse comitatus*).

6. *See* Cybersecurity Act of 2009, S. 773, 111th Cong., *available at* http://www.opencongress.org/bill/111-s773/text; *see also* National Cybersecurity Advisor Act of 2009, S. 778, 111th Cong., *available at* http://www.opencongress.org/bill/111-s778/show (known collectively as "Rockefeller Snowe Comprehensive Cybersecurity Legislation").

7. *See, e.g.*, Hands Off the Internet, http://dontregulate.org/.

defense risk management. For the DHS, coordination across all users of the "gov" domain will challenge traditional agency preferences for managing their own information technology. Nevertheless, we have at least launched the effort to coordinate the government cyber enterprise; the near term task is enhancing DHS capabilities.

Finally, for the various nongovernmental and commercial domains, perhaps we can get some ideas from the work of Elinor Ostrom, recently awarded the Nobel Memorial Prize in Economic Sciences. She has argued in her career that the commons tragedy can be solved from the bottom – individuals can organize on their own, and the government does not need to impose the rules from the top down.[8] She talks about limited purpose governmental enterprises that provide the guidance and standards (and perhaps assistance), but allow the participants to work out the rules.[9] In this concept of a true public/private cybersecurity partnership lies the space where the right balance of security and freedom is likely to be achieved.

8. *See* Elinor Ostrom, *A General Framework for Analyzing Sustainability of Social-Ecological Systems*, 325 SCIENCE 419 (2009).

9. *See* David Bollier, *Elinor Ostrom and the Digital Commons: From Net Neutrality to Wikipedia, the Nobel Winner's Ideas Are at Work Online*, FORBES, Oct. 13, 2009, *available at* http://www.forbes.com/2009/10/13/open-source-net-neutrality-elinor-ostrom-nobel-opinions-contributors-david-bollier.html.