THE CYBERSECURITY POLICY CHALLENGE

The Tyranny of Geography

ELAINE C. KAMARCK

Contents

Introduction	109
The Rise of Electronic Government	111
Problem #1: Diffusion of Responsibility between Government Organizations	114
Civil Liberty and Privacy Issues	118
The Public–Private Conundrum	120
People Issues	122
Conclusion	123
References	124

Introduction

It is not uncommon to begin a paper on the role of the government by imagining how surprised Presidents George Washington and Thomas Jefferson would be at the concerns of the day. But for cybersecurity one only has to go back to the first Clinton Administration to realize that it is a unique problem unlike anything government has ever faced. A search of major newspapers on LexisNexis, an information provider, finds *one* article that mentions cybersecurity prior to 1996, and that is a story of how credit card companies tried to go online and suffered near instantaneous security breaches. Part of the problem stems from the speed with which the Internet moved from a tool used

by a handful of researchers to trade information into something that is at the center of everything that modern people do. When I went to serve in the Clinton Administration in 1993, there was no World Wide Web. The Internet became available in the White House in 1996, but by the time I left government in 1997 I had never browsed the web. Today, hardly a day passes without me using it.

Because the Internet began benignly and grew rapidly, the government has played catch up and seems destined to continue to do so for quite some time. The American governmental father of cybersecurity, Richard A. Clarke, has a clear message in his best-selling book on the topic: America invented the Internet; it is the most wired country in the world, and hence, it is the most vulnerable—in spite of its sophistication. Clarke's insight has a historical distinctiveness that should not be overlooked. Technological advantages in warfare have always been associated with greater security for those who possessed them. But in the case of the Internet, technological advantage has simultaneously created vulnerability. In a brief amount of time the entire communications infrastructure of the nation has changed in ways that have made us more vulnerable to attack in spite of our economic and military advantages. Responding to these new threats poses policy challenges that are new to modern government.

But beyond being simply new, another reason that cybersecurity puts the government in uncharted territory has to do with geography, or in this instance, the absence thereof. From inception, government has relied on geography. Kings ruled kingdoms—areas of land with borders—sometimes imprecise, often disputed—but always defining the geography within which the state could act. In modern government geography exercises a tyranny over organization. The tyranny of geography defines the distinction between domestic and foreign, between nation and state, between state and town. Geography defines jurisdiction, “the power or right to exercise authority” per the *Merriam-Webster* dictionary. In modern government jurisdiction is implicit in everything from war between nation states to controversies between national and local authorities, as exemplified by tensions between the Federal Bureau of Investigation (FBI) and local police departments in the United States.

Cyberspace, however, transcends geography and herein lays the fundamental governmental problem. No one can put yellow police

tape around the cybercrime scene, and no one can define the battlefield. The absence of geography makes the traditional governmental tasks of protection and retribution especially difficult. It is also unclear who is in charge of protecting cyberspace. In the United States, the Department of Defense (DoD) created the first Cyber Command in 2010 while the FBI has traditionally taken jurisdiction in crimes that cross state lines as nearly all cybercrimes do. But when a cybercrime or cyber attack occurs, we have trouble finding out where the criminals are. We have established protocols, arrangements with other countries that allow us to extradite murderers, child molesters, and all sorts of other undesirables so that they can be brought to justice. But often we have no idea or cannot be sure where the cyber criminal is. If another country attacks us we know where the missiles come from and we can decide how to retaliate. But it is very difficult to know where hackers are. Sometimes we can pinpoint the country in which they sit but cannot determine whether the attack is an intentional attack by a government or an attack by a group of criminals who happen to be in a given country at a given time and who perhaps have also attacked sites in that same country.

This is why cybersecurity is a challenge unlike anything governments have encountered before. When we are able to establish jurisdiction, we are able to establish rules, laws, and accountability for adherence to the law—the three bedrock principles of modern democratic governance. In the absence of jurisdiction everyone is accountable and therefore no one is accountable. Other problems emerge from this underlying challenge to cybersecurity policy. Using the U.S. federal government as a primary example but also showing that these issues are common challenges to other information age countries as well, this chapter highlights diffusion of responsibility between government organizations and discusses three areas of complexity that flow from it: civil liberty and privacy issues, the challenge of public-private partnerships, and the people problem.

The Rise of Electronic Government

The Internet was created by the Defense Advanced Research Projects Agency (DARPA), an American government entity tasked with developing innovative technology for the military, and evolved from

there to a system used by the entire world. But less well known is that demand for computing was not only created by the United States but also by large, domestic, data-driven agencies like the Social Security Administration. Testimony to this fact was that when the year turned from 1999 to 2000, the infamous “Y2K” problem that was supposed to wreak havoc with computers around the world turned out to be largely an American problem, not a global one. The reason was that the U.S. government had practically single-handedly created the information age, and it alone, therefore, was the owner of “legacy” systems that were vulnerable to the Y2K problem.

By the time President Clinton and Vice President Al Gore came to office in 1993 the information age was already transforming the private sector. Gore, whose landmark legislation brought the Internet out of DARPA and into global use, was given the task of “reinventing government.” To do so, he was determined to use new information technologies to bring to the public sector the same large-scale productivity breakthroughs that had occurred in the private sector; hence, the term electronic government, or simply e-government, was born.

With lightning speed the Internet became critical to operations within government and to communications between citizens and government. As Gore led the Clinton Administration’s efforts to put the government online, it became evident that the Internet could promise huge savings to government and improved convenience to citizens. Initially most government agencies put information and forms online. But by the end of the Clinton/Gore Administration people wanted more than information—they wanted to be able to conduct transactions as well. For most of the world’s information age economies, the movement from “information” to “transactions” on the Internet was swift. As long as a country had a large number of citizens online and had a banked economy (i.e., not a cash economy), the move from office transactions to Internet transactions was relatively easy. New private sector entrants such as Ezgov.com and established corporations such as Microsoft and IBM also discovered a large new market opportunity in helping governments move from paper to web.

Research from the Pew Internet and American Life Project, which has been polling Americans about their use of the Internet since 2001, illustrates the increased use of e-government. Its 2010 poll found that

[M]any more Americans are now completing simple transactions with government than was the case in 2001. At that time, just 2% of online government users had paid a government fine online—now, 15% of all Internet users have done so. Similarly, 4% of online government users had applied for a recreational license online in 2001, a figure that has now grown to 11% of all Internet users. Renewing driver's licenses and auto registrations has also become much more common—from 12% of online government users in 2001 to one-third of all Internet users today.

The most common form of online government transaction has become tax filing, which has been growing steadily over the course of the past decade. In 2010, the Internal Revenue Service (IRS) reported that 99 million people used e-file in the United States, thus keeping up with a trend of steadily increasing use of the Internet for purposes of paying tax. In Sweden, about half the population declares their taxes online.

While America might have led the way, e-government is a global trend fueled by two powerful factors—public demand and cost. By 2007 the percentage of people who had used the Internet in their transactions with public authorities averaged 32% for citizens in the OECD countries. As younger tech-savvy citizens got to the age where they had to file tax returns and register motor vehicles they expected to be able to do this online, because they were doing most of their other transactions online—from buying clothes to meeting members of the opposite sex. On the government side of the equation, public sector leaders discovered that online transactions were much cheaper than offline transactions. Ezgov.com, an online solutions provider, estimated that postal or telephone transactions cost from 5 to 10 times more than an online transaction and that face-to-face transactions cost from 50 to 100 times more.

But as the rate of online transactions has grown so has the risk. It is one thing to hack into someone's Amazon.com account; quite another to hack into their tax or health records. And so, as e-government has expanded to keep pace with private sector dependence on the Internet so have the vulnerabilities of average citizens to cybercrime and the need for modern governments to provide some sort of coherent defense for its citizens. But in order to achieve good cybersecurity, the public sector must tackle several problems, all stemming from the tyranny of geography.

Problem #1: Diffusion of Responsibility between Government Organizations

The first recorded instance of computer espionage took place in 1986 and illustrated the problem with jurisdictional thinking when it comes to cybersecurity. The story is told in a 1989 book by Clifford Stoll called, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. The author, a graduate student managing computers at the Lawrence Berkeley National Laboratories, is asked to resolve a \$0.75 discrepancy in the lab's accounting system. As he tries to untangle this fairly minor issue, he discovers that someone is systematically hacking into or attempting to hack into U.S. military sites. As the saga unfolds and Stoll attempts to alert the authorities he is handed from one part of the government to another. The FBI initially cannot be interested in the problem because the amount of money involved is too small. The national security agencies are intrigued but do not know quite what to do. As Stoll is handed off from one federal agency to another, he encounters various parts of the government's national security apparatus—a culture shock for a self-described countercultural type. The story finally ends with the FBI coming back into the picture to arrest the hackers in Germany, an early illustration also of the fact that this is a global issue.

In the intervening years the governmental response to cyber threats has changed from the lackadaisical and somewhat quizzical attitude encountered by Stoll to one of intense interest, not to mention intense funding. But the cacophony of governmental entities in the game persists because in cyberspace the government is playing both offense and defense.

In the United States, the offense is and has been handled, not surprisingly, by the DoD and the National Security Agency (NSA), both of which have been involved in this area for a long time. For example, according to Clarke's new book, *Cyber War: The Next Threat to National Security and What to Do about It*, the first class of officers trained in cyber war graduated from the National Defense University in 1995. In 1996, cryptome.org, a military news website, reported that the Pentagon published a report of the Defense Science Board Task Force on Information Warfare Defense, which was one of the earliest to identify the possibilities and vulnerabilities of the United

States to information warfare. Also in 1996, the Central Intelligence Agency (CIA) was already dealing with the cyber world through its advanced technology panel. But within the U.S. federal government no agency has been as preeminent as the NSA, which, as the nation's premier organization for electronic spying, has had the technological and legal authority to explore infiltration of the Internet for intelligence purposes. Its long involvement and significant expertise has given it enormous capacity which is why General Keith Alexander assumed a dual position as Director of NSA and Commander of the U.S. Cyber Command, formed in 2010. The other reason that NSA is the preeminent government player in this area has to do with money. Although the portion of the cyber budget at DoD is difficult to determine because so much of it is for "black" or cybersecurity activities that are highly classified, most sources put it at somewhere around \$2.3 billion—a number that dwarfs spending on the nonmilitary side of the budget.

The defensive side of cybersecurity has been located in the Department of Homeland Security (DHS) ever since it was created in the wake of the 9/11 attacks, a result of combining 22 existing agencies into one. The perception that the defensive, or domestic, side of the government's cybersecurity operation was weak has been reinforced by an overall impression that DHS was weak. In its early years, DHS was known in government as a dumping ground for mediocre civil servants. On the political side, DHS was known as the place where the Bush Administration placed people it owed political favors without regard to their preparation for the job. Colonel Robert Stephen, who was brought into the White House to work for then homeland security advisor Tom Ridge (whom he followed to DHS when the new department was created), recalls the early days of DHS: "The NSA was off doing its own thing, DoD was doing its own thing. Their two ships never crossed paths. There was a lot of contention between FBI and DHS over this.... We brokered a truce in the 2004 time frame [because] everyone was setting up their own cyberspace. DHS was the newer and weaker kid on the block" (Interview with Author, 2010).

The status of DHS in this area began to change in 2007 as a result of presidential attention. Again, according to Stephen (2010):

To be honest... none of it mattered until 2007 (late spring or early summer) when the Office of the Director of National Intelligence requested briefing time with President Bush and rolled in with a very scary cyber briefing. Bush got very interested in this after that and did a quick study. Within a few months after that at a briefing with the National Security Telecommunications Advisory Committee—Bush came in for 45 minutes and talked in depth about the cyber problem and pinged 30 CEOs in the room. ...When the President gets involved... first lots of money appears. ...From that moment on it became an interagency frenzy.

By 2008, President Bush's attention to cybersecurity was being felt throughout the government. Michael Chertoff, Secretary of DHS, made it one of his top priorities for 2008, admitting to reporters in a *USA Today* article that "It's the one area in which I feel we've been behind where I would like to be" (Wolf, 2008, p. 6A). Bush's budget proposed a 10% increase in cybersecurity funding. The increased attention coincided with an increase in reported security breaches to DHS and reports that Estonia's largest bank had been shut down for 3 weeks in 2007, a victim of cyber attacks.

President Obama came into office promising that he would put cybersecurity on center stage. One of the first things he did was to task Melissa Hathaway of the Office of the Director of National Intelligence to conduct a comprehensive 60-day review to assess U.S. cybersecurity. The plan, formally known as the "Cyberspace Policy Review," was released on May 29, 2009. The very first recommendation was to appoint an official responsible for coordinating the nation's cybersecurity policies and to create an National Security Council (NSC) directorate devoted to the interagency coordination of those issues. On January 6, 2010, the White House announced that Georgia Tech professor Howard Schmidt, a former Microsoft official with decades of experience in the field, would assume the role of cyber czar. His tenure has illustrated the divisions within government, reflected in the difficulties DHS has had in recruiting and retaining leadership and in the ongoing disputes within the government between the domestic and national security sides. For instance, Seymour Hersh, a veteran journalist, reported in a 2010 article in *The New Yorker* that the Director of the National Cybersecurity Center Rod Beckstrom had resigned, stating that DHS's cybersecurity efforts

are “controlled” by the National Security Agency. Beckstrom is not the first DHS official to resign in frustration and thereby prompt attempts at solving the underlying problem of who’s in charge of what. In 2005, Amit Yoran, the very first director of cybersecurity, left amidst speculation that he was frustrated at the lack of importance put on cybersecurity at the DHS. Michael Chertoff, the then Secretary of DHS, responded that summer by announcing the creation of the position of Assistant Secretary for Cybersecurity and Telecommunications. After Beckstrom’s departure the Secretary of Defense Robert Gates and the Secretary of Homeland Security, Janet Napolitano signed a Memorandum of Agreement, published in October 2010, that would place DoD analysts at the National Cybersecurity and Communications Integration Center (NCCIC) and would place DHS personnel at NSA. This was widely praised as an important step in recognizing the difficulties inherent in trying to separate cybersecurity issues by organization. Nonetheless, some believe that this will not be enough and that the only solution will be to place cybersecurity in its own separate organization. A 2010 report by the Center for Strategic and International Studies (CSIS), a Washington think-tank that conducted President Obama’s 60-day review of cybersecurity policy, stated: “Although the administration created a cybersecurity coordinator and a new office, we still believe that the nation will ultimately need something like the Office of the U.S. Trade Representative to lead and coordinate federal policy for what has become a central element of national security and economic life” (p. 6).

For the time being, however, the U.S. federal government seems to have opted for a decentralized approach to cybersecurity where the DoD controls offense and defends the dot-mil domain space and where DHS is responsible for the dot-gov domain space and attempts to coordinate security with the private sector. In practice this means leaving large portions of cyberspace to their own devices when it comes to security. This is similar to the current European approach where there is a strict division of labor between the civil and military approaches to cybersecurity, again leaving large parts outside of government domain. Specifically, European Union (EU) policy is developed only in regard to civilian defense of cyberspace, and the organization’s member states are responsible for military operations.

Coordination of Western military response at the international level, another topic of diffusion of responsibilities, is primarily addressed through NATO's Cooperate Cyber Defense, located in Tallinn, Estonia, which was created in response to the 2007 cyber attacks on that country.

Those who feel that the current level of government involvement is not sufficient face major obstacles in attempting greater coordination and centralization—concerns about privacy and civil rights, difficulties in getting cooperation from the private sector and the problem of attracting talented information technology (IT) personnel to government service.

Civil Liberty and Privacy Issues

Civil liberty and privacy issues have been at the center of the government's attempts at cybersecurity since the very beginning and complicate efforts to achieve greater cooperation and centralization. In the United States, the involvement of NSA continues to rouse suspicions among privacy advocates. NSA is tasked with electronic spying on a global level but is prohibited from spying on U.S. citizens. In a world where jurisdiction could be defined by geography this was not a problem—in today's world it is. This dilemma came up early in the history of U.S. government involvement in cybersecurity. In the Carter Administration, the Department of Commerce was made responsible for the protection of unclassified computer information. But a 1984 executive order by President Reagan shifted responsibility for computer security to the DoD and the NSA. The outcry from the private sector, civil libertarians, and privacy advocates was swift. They did not want domestic computer systems coming under the Defense establishment. As a consequence, in 1987 Congress passed the Computer Security Act, which placed responsibility for the federal government's computer security in the hands of the National Institute of Standards (NIST) at the Department of Commerce while giving the DoD and NSA authority over classified computers.

By the mid 1990s, as security issues moved from securing the federal government's computers to securing a network that was dominating all aspects of society, the preferred position of those concerned with privacy was to advocate a "hands-off" policy. Government

intervention, it was argued, would only ruin the Internet which was a truly self-regulating system. This laissez-faire attitude toward the Internet was so widely accepted that when Ira Magaziner, author of the ill-fated Clinton health care plan, was given a second governmental assignment—running a panel to look at governance of the Internet—he concluded that government should refrain from regulating the Internet. The irony was duly noted. The same person who had sought to get the government into the business of health care took a big step away from that position when confronted with the Internet.

Unfortunately, terrorism, like cyber terrorism, defies the jurisdictional lines upon which modern government was formed where spying on fellow Americans was under the jurisdiction of the FBI and the court system; the national security agencies were supposed to stay away from Americans and from the homeland. None of this mapped very well to the terrorist and the electronic worlds, both of which arrived in the United States at about the same time. Thus, in response to the events of 9/11, President Bush created the Patriot Act that authorized NSA surveillance of American telephone and Internet communications without prior Foreign Intelligence Surveillance Act (FISA) approval. As the involvement of the big telecommunications companies in this arena came to light, the Electronic Frontier Foundation and the American Civil Liberties Union took the big companies to court. The cases were eventually dismissed in part because FISA was revised to make it somewhat easier to conduct electronic surveillance while building in safeguards for American citizens. Spying on fellow Americans now involves a complex set of legal procedures and a heavy dose of probable cause that a crime was in the works.

Although the anger and court cases over electronic surveillance are no longer front-page news, they left a powerful legacy of concern over privacy, most of which has its origin in the heavy involvement of NSA in cyberspace. The problem is tricky because while NSA has perhaps the best technical ability in the government, it is primarily a spy agency. And so in 2009, Amit Yoran, the first director of the National Cyber Security Division during the Bush Administration, testified before Congress as follows: “In news reports and discussions among privacy and civil liberties groups the role of the NSA in monitoring or defending domestic private networks is debated. Should such intelligence

programs exist, DHS should be very careful to distance itself from participation, support or engagement in these activities.”

By the time the Obama Administration issued its 60-day review in early 2010, privacy issues were not much closer to being resolved than they had been nearly 30 years before in the Reagan Administration. Out of the 10 near-term action items proposed in the review, two dealt specifically with privacy. The first advocated that a privacy and civil liberties official be assigned to the NSC cybersecurity directorate. The second called for building a program that addressed privacy, civil liberties, and privacy-enhancing technologies.

In contrast to the hands-off approach of the United States, the European Union takes an active role in regulating data protection with most policies in this area concerning privacy as in the protection of personal data. With a community of 600 million people across 27 member states, a number of initiatives cover data protection and privacy, including, perhaps most notably, the Data Protection Directive 95/46/EC, which offers strong protection of individual data. A formal review to update privacy legislation was started in 2009 in an effort to maintain protection while improving data-sharing. Like its American counterparts, European telecommunications companies have found themselves in the middle of the issue as they would need to breach personal data to properly address risk.

The fact of the matter is that this issue has no easy answers. To further complicate matters, in addition to the public at large and policy makers, privacy issues are also important to the private sector, which is often at the center of the debate.

The Public–Private Conundrum

Among the primary obstacles to cybersecurity has been and remains the fact that the bulk of IT systems vulnerable to attack are in the private sector. It was clear from the beginning that security enhancements to private systems would be expensive, cut into the bottom line, and compromise effectiveness. And no one was quite sure that this was even necessary. Typical of a debate that has not really been solved was a headline from *Kiplinger Business Forecasts*, on January 15, 2002, that read, “Keeping Systems Safe From Cyber Bugs Can Cut Productivity.” When U.S. Republican Senator Robert Bennett

of Utah proposed that the Securities Exchange Commission (SEC) adopt rules requiring public companies to disclose their readiness to meet cyber threats, the business community mobilized to argue that cybersecurity should be treated as a risk factor *where appropriate* but that it should not be an entirely new disclosure category, an argument that won out.

President Obama's 60-day review admitted that "the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk." The report also acknowledges private sector concerns beyond the bottom line. In addition to being reluctant to make major investments in cybersecurity, businesses are cautious about sharing information about security breaches with the government for fears that such information can be subject to the Freedom of Information Act, lead to public disclosure, and ruin trust in a company or reveal trade secrets to its rivals. Further, businesses loathe disclosure of proprietary information and too much interaction with the government can lead to unanticipated regulatory actions. In other words, there are few incentives for the private sector to engage in the sorts of partnerships that are put forward as a solution to these problems. In spite of legislation such as the Trade Secrets Act and the Critical Infrastructure Information Act, both designed to deal with the problems posed by the Freedom of Information Act disclosures, private sector skepticism remains. All too often businesses prefer to defend themselves without the government.

Even in the case of large infrastructure companies, who are most vulnerable to attacks, the government has to tread lightly. In the United States, for instance, NSA is developing a program called "Perfect Citizen," a digital surveillance program to detect cyber attacks on private companies such as the electricity grid, dams, and nuclear power plants. But as the following quote from the *Wall Street Journal* (Gorman, 2010) indicates, the program is not mandatory: "While the government can't force companies to work with it, it can provide incentives to urge them to cooperate, particularly if the government already buys services from that company, officials said" (p. 3).

The tentativeness with which government is moving into the area of critical infrastructure is not limited to the United States. In

Great Britain, the Government Communications Headquarters, the UK's version of NSA, is seeking to broaden its mandate to watch for signs of attack on private systems. According to the *Computer Business Review*, an industry publication, the Prime Minister met with heads of major companies to discuss the plan but the government was careful to deny that the plan has any privacy implications.

Official pronouncements about the importance of public-private partnerships in the area of cybersecurity are ubiquitous. But the problem remains. As long as the private sector feels it can defend itself against attack or that it can quickly recover, the risks of greater government involvement will seem high. Government has been loathe to mandate security improvements that might be deemed too expensive, and it has been reluctant to force its involvement on private sector entities such as utilities and power plants where the consequences of cyber attacks can be catastrophic.

People Issues

It is generally difficult for the public sector to attract and keep talent in the area of cybersecurity because top IT professionals are always in demand by the private sector, whether the economy is good or bad. To deal with the issue in the United States, DHS Secretary Janet Napolitano recently received exemptions from civil service hiring and wage scales in order to hire 1,000 cybersecurity experts. But in spite of the exemptions and in spite of studies by respected institutions such as the National Academy of Public Administration urging new compensation structures for IT professionals, the government has trouble filling these IT posts. "We're all fighting for the same resources. We don't have thousands of unemployed security professionals," said Patricia Titus, chief information security officer (CISO) for information technology firm Unisys and former CISO at the Transportation Security Administration in a 2010 article in *SFGate.com* (Cabrera, 2010, p. 2). "Good IT professionals are still employed and trying to entice them from private sector into the government is going to be difficult."

The people problem was front and center in President Obama's 60-day review, which argued for new policies to attract cybersecurity

expertise and improve retention. For example, while the review noted a small measure of improvement in recruitment, it acknowledged the time needed for security clearances remains inadequate. To deal with retention, the review promoted the idea that employees should be able to build their professional portfolios beyond a single agency, suggesting “Shared training and rotational assignments across agencies and potentially with the private sector would not only be efficient, but would promote beneficial cross-fertilization and the building of professional networks” (Cyberspace Policy Review, p. 15).

The people problem in the federal government exists at both the civil service and political levels. At the civil service level it is a subset from the bigger problem that the federal government suffers from an antiquated personnel system that is bad at attracting and retaining highly skilled workers. At the political level talented IT leaders have so many more lucrative opportunities outside of government that there is little incentive for them to stay on and fight the bureaucratic battles. The leadership problem is directly connected to the problems outlined above; the lack of clarity about the government’s role in cyberspace means that, as we’ve seen, talented leaders in this field can easily feel that they are spinning their wheels and that they could make more of a contribution outside the government.

Conclusion

There is no doubt that public sector organizations throughout the modern world are more aware and more capable of dealing with threats to cyber infrastructure today than ever before. More money is being spent and more vulnerabilities are being identified. But in the nearly three decades since the U.S. federal government has been concerned with protecting first its own computers and then the Internet, the challenges of dealing with cybersecurity have not changed much.

At the heart of the cybersecurity policy challenge is the traditional government geographical division into foreign and domestic issues, which is now obsolete. A cyber attack can be both and the organizations needed to defend cyber infrastructure will probably involve both as well. Cybersecurity is one of the biggest challenges governments have ever faced—in part because there’s never been a challenge like it.

Government has been organized around physical geography for centuries but the cyber threat is borderless and challenges the domestic and the national security sides of the government to achieve a seamless architecture of cooperation. Up until now both the public and private sectors have simply dealt with challenges as they have come up. While some of them have been embarrassing, they have been fixed, usually in an acceptable amount of time. In other words, so far the system of cybersecurity has largely been able to cope with the threat.

But that is because so far the threat has not been “existential”—to borrow a phrase from national security policy. There is still debate about the potential impact of cyber attacks on physical security but until it is settled we will continue to live with a somewhat cautious government involvement that is influenced by the original culture of the Internet—“open, untrammelled, ... the Wild West...a self-organizing community led by private action where governments should play only a limited role,” as described by the CSIS report. Until the assumptions inherent in the original culture of cyberspace prove to be obsolete, we will be left with a cybersecurity architecture that is suboptimal.

References

- Author's interview with Colonel Robert Stephen, October 19, 2010.
- Cabrera, A. M., “Demand Keeps Growing for Cyber Security Workers,” April 2, 2010, in SFGate.com, p. 2.
- “CCHQ to Monitor Private Networks for Cyber Attacks,” by CBR Staff Writer, *Computer Business Review*, March 29, 2011.
- Clarke, R., and Knake, R., *Cyber War: The Next Threat to National Security and What to do About It*, (Harper Collins), p. 34.
- “Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th President,” Commission Cochair, Reps. James R. Langevin and Michael T. McCaul, Scott Charney and Lt. General Harry Raduege. http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf.
- “Cyberspace Policy Review,” The White House. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
- Gorman, S., “U.S. Plans Cyber Shield for Utilities, Companies,” *The Wall Street Journal*, July 8, 2010.
- Hersh, S., “The Online Threat: Should We Be Worried about a Cyber War?” *The New Yorker*, November 1, 2010. http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh#ixzz15AvfyXiq.

- McKenna, C. "Bill to Create Assistant Secretary for Cybersecurity at DHS Delivered to Full House," April 22, 2005. Digitalcommunities.com/articles/Bill-to-Create-Assisant-Secretary-for.html.
- Moscaritolo, Angela, "Policy Makers Debate White House's Role in Cybersecurity," *SC Magazine*, April 28, 2009, <http://www.scmagazineus.com/policymakers-debate-white-houses-role-in-cybersecurity/article/131513/>.
- Nakashima, Ellen, "U.S. Cyber-Security Strategy Yet to Solidify," *The Washington Post*, September 17, 2010.
- OECD, *The Future of the Internet Economy, A Statistical Profile*, 2008.
- Office of the Under Secretary of Defense for Acquisition and Technology, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)," <http://cryptome.org/iwd.htm>.
- Smith, A. "How Americans Use Government Websites." Pew Internet and American Life Project at: <http://www.pewinternet.org/Reports/2010/Government-Online/Part-One/How-Americans-use-government-websites.aspx>.
- Stoll, C., *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Simon & Schuster Pocket Books, 1989.
- Testimony of Amit Yoran before the House Homeland Security Committee, "Reviewing the Federal Cybersecurity Mission," March 10, 2009.
- Wolf, Richard, "Bush Pushes Cybersecurity; President Wants to Raise Funding to \$7.3 Billion," *USA Today*, March 14, 2008.