I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Cyber Policy: Institutional Struggle in a Transformed World

TERRENCE K. KELLY AND JEFFREY HUNKER

I. INTRODUCTION

When it comes to cyber security, the world today is not the future that U.S. policy promised when cyber security first appeared on the national agenda well over a decade ago.[1] The great advancements envisioned then have almost universally not come to fruition. In 2000, while announcing an unprecedented $2 billion in federal cyber security funding at an unprecedented White House conference on cyber security, President Clinton noted that: "[Cyber attacks are] just a replay of what always happens when there is a new way of communicating, a new way of making money[. T]hroughout human society, there will always be someone who tries to take advantage of it, we will figure out how to deal with it."[2] Confidence that, with a bit of focus, adequate cyber security would be achieved appears almost quaint now. Instead, it is unlikely that the United States can create and implement effective cyber security policy.

The cyber threat that was then mostly posed by isolated teenage hackers has now transmogrified into one posed by highly sophisticated criminal organizations with growing nation-state capabilities.[3] Consider these relatively recent developments:[4]

---

[1] PRESIDENT'S COMM'N ON CRITICAL INFRASTRUCTURE, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 5 (1997), *available at* http://*www.fas.org/sgp/library/pccip.pdf*.

[2] Deborah Tate, *Clinton–Internet Security*, FEDERATION OF AMERICAN SCIENTISTS (Feb. 2, 2000), http://www.fas.org/irp/news/2000/02/000215-hack2.htm.

[3] MISHA GLENNY, DARK MARKET: CYBERTHIEVES, CYBERCOPS AND YOU 266 (2011).

- Cyber war is now a reality. In the fall of 2010, the world learned about the Stuxnet worm—a highly sophisticated computer attack tool that disrupted centrifuges processing nuclear fuel for the Iranian nuclear bomb program.[5] This event was the first tangible illustration that cyber attacks can disrupt not just computers, but also physical processes in the real world. While Stuxnet was certainly a national effort, no nation took credit, though the U.S. and Israel are reported to be suspects.[6] Perhaps ironically, in the spring of 2011, the U.S. Defense Department declared that cyber attacks could be considered an act of war.[7] We have entered a new—and very messy—age where cyber attacks without clear origin can cause physical destruction and eventually, even if unintended, start killing people.

- Political "hactivism" threatens to become another major force for disruption in cyberspace. In the fall of 2010, the release of sensitive, stolen U.S. government cables by WikiLeaks demonstrated U.S. cyber insecurity and sparked a vigilante war reminiscent of the Wild West.[8] First, the WikiLeaks site was shut

---

[4] JEFFREY HUNKER, CREEPING FAILURE: HOW WE BROKE THE INTERNET AND WHAT WE CAN DO TO FIX IT 40 (2011).

[5] *Securing Critical Infrastructure in the Age of Stuxnet: Hearing before S. Comm. on Homeland Sec. and Gov't Affairs*, 111th Cong. 29 (2010) (opening statement of Chairman Lieberman) (discussing Stuxnet, the worm that "demonstrates to us the extraordinary capacity that a worm could have to disrupt absolutely critical infrastructure.").

[6] *See* William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. Times, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all.

[7] U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

[8] *WikiLeaks Defies U.S., Releases Embassy Cables*, CBS NEWS, Nov. 30, 2010, http://www.cbsnews.com/2100-202_162-7096946.html (last visited Apr. 7, 2012).

down briefly by denial-of-service attacks launched by unknown persons.[9] In return, "hacktivist" groups like Anonymous attacked U.S. government sites, as well as sites of companies that had distanced themselves from WikiLeaks, like Amazon, PayPal, and MasterCard.[10] Anonymous has since broadened and popularized the notion of launching cyber attacks against governments and corporations considered politically or socially repugnant.[11] Actually, the term "hactivism" belies the potential destructiveness of this new development. Disruptive political action in cyberspace may soon morph into destructive attacks.

- Quietly, but with serious consequences, the Internet's model of "governance by no governance" is failing to keep the Internet running. Quite simply, the Internet has run out of IP addresses.[12] While it will take some time

---

[9] *Id.*

[10] *See* Cassell Bryan-Low & Sven Grundberg, *Hackers Rise for WikiLeaks*, Wall St. J., Dec. 8, 2010, http://online.wsj.com/article/SB10001424052748703493504576007182352309942.html; Richard Allen Green & Nicola Hughes, *'Hacktivist' for Good Claims WikiLeaks Takedown,* CNN, Nov. 29, 2010, http://articles.cnn.com/2010-11-29/us/wikileaks.hacker_1_wikileaks-computer-hacker-cyber-attack?_s=PM:US; Olga Khazan, *Anonymous Defaces Security Firm's Web Site in Retaliation for Arrests*, Wash. Post, March 7, 2010, http://www.washingtonpost.com/business/technology/anonymous-defaces-security-firms-web-site-in-retaliation-for-arrests/2012/03/07/gIQAonKqwR_story.html.

[11] *See, e.g.*, Jesse Emspak, *Anonymous Threatens to Post Info on Bradley Manning's Guards*, Int'l Bus. Times, Mar. 10, 2011, *available at* http://www.ibtimes.com/articles/121434/20110310/wikileaks-bradley-manning-anonymous-threats.htm; *Anonymous Activists Target Tunisian Government Site*, BBC News, Jan. 4, 2011, http://www.bbc.co.uk/news/technology-12110892; Peter Overby, *Billionaire Brothers In Spotlight In Wis. Union Battle*, NPR, Mar. 1, 2012, *available at* http://www.npr.org/2011/02/25/134040226/in-wis-union-battle-focus-on-billionaire-brothers.

[12] Dylan Tweney, *No Easy Fixes as the Internet Runs Out of Addresses*, WIRED, Feb. 3, 2011, *available at* http://www.wired.com/epicenter/2011/02/internet-addresses/all/1.

for this problem to work its way through the system, no one sees a happy ending unless there is a universal adoption of IPv6, an updated technical protocol that has been available for years.[13] A massive tragedy of the commons is now underway, since no single Internet service provider finds it in its interest to adopt the new protocol, despite it being in the common interest.[14] As of this writing, adoption of IPv6 is around 0.4% for all Internet routers (i.e., four out of every 10,000 routers).[15]

- The sophistication and scale of cyber crime continue to grow. Every few months brings the latest "worst ever cyber theft," such as the successive thefts of over 100,000,000 user accounts from Sony in April 2011.[16]

Explaining every facet of the manifest failure of U.S. and G7 cyber security policy to ensure a safe cyber space is beyond our scope. Our thesis is that a fundamental element in this failure is that cyber security challenges the institutional capabilities of governments in general and, for purposes of this paper, the U.S. Government in particular. The prerequisites for effective public policy have not been met with respect to cyber security and critical infrastructure protection.

---

[13] *Id.*

[14] Richard Clayton, *Internet Multi-Homing Problems: Explanations from Economics*, *in* ECONOMICS OF INFORMATION SECURITY AND POLICY 67, 71 (Tyler Moore, Christos Iannidos & David J. Pym eds., 2010).

[15] *IPv6 Statistics*, GOOGLE, http://www.google.com/intl/en/ipv6/statistics (0.38% of users would access Google over IPv6 if Google had an IPv6 address as of January 6, 2012) (last visited Apr. 7, 2012).

[16] Charles Arthur, *Sony Suffers Second Data Breach with Theft of 25m More User Details*, GUARDIAN UK, May 3, 2011, http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment.

This thesis originated at a symposium organized at The Ohio State University in April 2011.[17] The objective was to focus discussions among a wide range of experts and scholars from different perspectives on two objectives: first, to move beyond generalities in specifying the roles and responsibilities that both the public and private sectors would have to shoulder in order for the U.S. to share global leadership in cyber security; and second, to broaden the community of researchers, policy makers, and professionals from around the globe who work on cyber security.[18]

Our goals in this Article are to set out a framework for the public policy-making processes germane to cyber security policy, demonstrate the deficiencies that exist in cyber security policy, and make some modest recommendations on making more effective policy in this domain.

II. THE PECULIAR PROBLEM OF CYBER SECURITY

A number of factors make the development and implementation of public policy for cyber security simultaneously complex,[19] important, and contentious:

- By design, the Internet lacks any degree of centralized control. It does not have anything but a very loose, voluntary governance system. It differs markedly from traditional "circuit switched" telephony, the other major global communications network.[20] Relatively few

---

[17] Symposium, *Cyber Security: Shared Risks, Shared Responsibilities*, I/S: A Journal of Law and Policy for the Information Society Symposium (Apr. 1, 2011), http://cybersecuritycommunity.org.

[18] *Id.* at http://cybersecuritycommunity.org/?page_id=3.

[19] Complexity is an engineering term. Complexity involves unfamiliar, unplanned, or unexpected linkages between actions (of whatever sort), and which are either not visible or not immediately comprehensible. 'Complicated' involves a high multiplicity of 'linear interactions' which in and of themselves are understandable. Complicated systems can be understood; complex systems often produce unexpected results. CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH RISK TECHNOLOGIES 72-79 (1999).

[20] A "circuit switched" network is a network in which there exists a dedicated connection. A dedicated connection is a circuit or channel set up between two nodes so that they can communicate. After a call is established between two nodes, the connection may be used only by these two nodes. When the call is ended by one of the nodes, the connection is canceled. *Understanding Telephony Concepts and Components*, MICROSOFT EXCHANGE

players own and operate telephony globally. Many operators are national governments, yet telephony has effective, if sometimes criticized, governance through the International Telecommunications Union.[21]

- Computers and computing systems are rife with vulnerabilities to both accidental failure and deliberate attack. These vulnerabilities are, in general, often poorly understood and difficult to correct.

- Most cyber networks are in private sector hands, especially those in the U.S., yet increasingly large parts of cyber space are outside of the U.S.[22] U.S. government-controlled networks are a very small part of cyber space.[23]

- Cyber space is interconnected and interdependent, with the interdependencies being difficult to identify, understand, and analyze.[24]

- In the U.S., there is strong resistance to any form of direct government regulation of any aspect of cyber space, including software,

---

SERVER (last modified Aug. 22, 2011), http://technet.microsoft.com/en-us/library/bb124606.aspx.

[21] INT'L TELECOMM. UNION, MODULE 1: REGULATING THE TELECOMMUNICATIONS /ICT SECTOR 1 (2012), *available at* www.ictregulationtoolkit.org/en/SectionPDF.3096.html.

[22] CYBERSPACE POLICY REVIEW, ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2011), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[23] Bennie G. Thompson & Sheila Jackson-Lee, *Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve*, U.S. GOV'T ACCOUNTABILITY OFFICE 7 (July 10, 2007), *available at* http://www.gao.gov/new.items/d07706r.pdf.

[24] Rindaldi et al., *Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies*, IEEE CONTROL SYSTEMS (Dec. 2001).

> hardware, and network management. The challenges to creating good cyber security policy come from many sectors of society, such as privacy advocates, business interests, libertarians, and technical purists who simply do not want the government tinkering with the Internet.[25] Concerns about federal government-enacted cyber security policy range from privacy considerations,[26] to the role of government in society, to statutory considerations regarding the roles government agencies can play in domestic cyber activities.

Creating effective public policy is hard in general, and, for controversial issues in which there are strong constituencies for and against the policy envisioned, agreeing upon policy can take years, if not decades (e.g., the Clean Air Act).[27] Because the government does not own the Internet, other major elements of cyberspace, or most of the critical infrastructures that depend on the Internet, and because there are strong incentives for many groups to resist measures that would help secure the Internet,[28] efforts to create and enforce cyber security policy are especially difficult.

---

[25] This debate is far reaching and involves many parties. Representative sources include Carl Bildt, *Keep the Internet Free*, N.Y. TIMES, Oct. 11, 2005, http://www.nytimes.com/2005/10/10/opinion.10iht-ebbildt.htm; *ACLU Joins AT&T, Google, and Privacy Groups to Urge Updates to Privacy Law*, AM. CIVIL LIBERTIES UNION, (March 30, 2010), http://www.aclu.org/technology-and-liberty/aclu-joins-att-google-and-privacy-groups-urge-updates-privacy-law; JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008); Kevin Marron, *Guarding Consumer Privacy Isn't Just The Law -- It Could Keep Your e-Business From Crumbling*, THE GLOBE AND MAIL (Toronto) (last updated Mar. 21, 2009), *available at* http://www.theglobeandmail.com/news/technology/guarding-consumer-privacy-isnt-just-the-law----it-could-keep-your-e-business-from-crumbling/article509758.

[26] EPIC, for example, has contributed to several white papers and articles on privacy considerations. *Cyber Security Privacy Practical Implications*, EPIC, http://epic.org/privacy/cyber security (last visited Apr.7, 2012).

[27] For example, the Clean Air Act was enacted in 1970, but it was not effective until it was amended in 1990, alleviating some of the original Act's negative economic effects. *See* Robert M. Friedman et al., *Urban Ozone and the Clean Air Act: Problems and Proposal for Change*, THE FEDERATION OF AMERICAN SCIENTISTS: OFFICE OF TECHNOLOGY ASSESSMENT ARCHIVE 1 (Apr.1988), *available at* http://www.fas.org/ota/reports/8841.pdf.

[28] EPIC, *supra* note 26.

The general framework of cyber security policy across the G7 tends to be led and shaped by the United States, which has had formal national policies in place since 2000.[29] While these policies have been refined and revised through implementation, the core elements of U.S. and G7 cyber security policy have remained essentially unchanged over the past decade. These core policy goals are to:

- pursue research and development for more effective security and reliability solutions;
- ensure the security of federal systems, notably those outside of the traditional national security envelope, both for their own sake and as a model for non-federal systems (those inside the national security envelope are governed by other protocols);
- promote domestic and international initiatives in cyber law enforcement coordination; and
- build public-private partnerships for voluntary action in order to ensure the security of select key "critical infrastructures."

This means that G7 governments have to secure their own non-national security networks, create new organizations and new linkages with the private sector, and fuse aspects of their criminal and defense organizations, while key parts of the private sector take on national security responsibilities[30] perhaps unequalled since the 18th century British East India Company.[31]

---

[29] A large number of U.S. national policies relating to cyber security (and a related topic, critical infrastructure protection) have been prepared since 2000; *See, e.g.*, WHITE HOUSE, NATIONAL PLAN FOR INFORMATION SYSTEMS PROTECTION, VERSION 1.0 (Jan. 2000); WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003); WHITE HOUSE, COMPREHENSIVE NATIONAL SECURITY INITIATIVE (NSPD 54/HSPD-23) (2008); DEP'T OF HOMELAND SEC., NATIONAL INFRASTRUCTURE PROTECTION PLAN: PARTNERING TO ENHANCE PROTECTION (2009); WHITE HOUSE, CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009). A fuller list of policy reports is contained in CREEPING FAILURE, *supra* note 4, at 120–21.

[30] CYBERSPACE POLICY REVIEW, *supra* note 22, at 17–21.

[31] The British East India Company was one of the first joint stock companies, created by royal charter by Queen Elizabeth in 1600 with a monopoly on trading beyond the Cape of

III. WHAT MAKES THE GOVERNMENT "COMPETENT" IN A POLICY AREA?

Some believe that government is the problem, not the answer. But if we assume that public policy can be effective and should be developed in areas of national interest that cannot be handled by private individuals, organizations, or corporations, then there are some factors that shape whether government can effectively create and implement public policy. These include:

1. Clear statements of policy goals and acceptable approaches to achieving these goals, derived from consensus among key stakeholders;

2. Authorities that permit government to act; and

3. Fiscal and human resources to implement the proposed policy.

Even in clear-cut circumstances, policy formulation and implementation can be difficult. In the case of national defense, which putatively should be one of the easiest areas for policy makers to create policies and implementing strategies, one need only look to issues facing large military programs. For example, the debate over whether to buy an alternate engine for the F-35 fighter[32] demonstrates that, even for important issues in which basic policy is agreed upon, like the need for a fifth-generation fighter, implementation can be very controversial.

Good Hope and the Straits of Magellan. It was created to compete with the Dutch East Indies Company, of similar organization. The British East India Company started with 125 shareholders (eventually to grow to 3000), who annually elected a set of Directors to run the company. In the 1700's the East India Company obtained a virtual monopoly on trade with India, and gained the right to acquire territory, coin money, command fortresses and troops, form alliances, make war and peace, and administer civil and criminal jurisdiction. Stated simply, as a private company it essentially ran India until 1858, when a revolt of its native troops (the Sepoy Rebellion) resulted in Britain purchasing India from the British East India Company, which shortly later was dissolved. THE ENCYCLOPEDIA BRITANNICA VOL. VIII, *East India Company* 834, (11th ed., New York, University Press, 1910).

[32] *See* Jeremiah Gertler, *F-35 Alternate Engine Program: Background and Issues for Congress*, CONG'L RESEARCH CTR., Jan. 10, 2012, *available at* http://www.fas.org/sgp/crs/weapons/R41131.pdf.

In other cases, we have seen important national challenges for which policy was created without ensuring that adequate resources would be in place to implement it. This, in turn, creates challenges when the policy is enacted. For example, as the civilian efforts to rebuild Iraq were being developed and implemented in 2003, the U.S. government did not consult with its own personnel experts in the Office of Personnel Management regarding adequate staffing.[33] This resulted in the Coalition Provisional Authority, which governed Iraq until the Iraqi government could be put into place, never having enough people or people with the right skills to succeed at the tasks it faced.[34]

If government is to effectively implement policy, it must be organized to do so, and so we offer one additional prerequisite for effective public policy:

4. Government organizations that have the capabilities, including organizational structure, skills, knowledge, relationships within government and with the private sector, and the capacity required to implement policy.

Organizational capability and capacity are not just functions of funding. They require organizational culture and an adequate foundation of personal and institutional relationships, tacit and explicit knowledge, and capabilities and functions that take a long time to develop. The importance of this fourth principle is well-illustrated by the challenges the Department of Homeland Security faced in its creation.[35]

There can be understandable confusion between the third and fourth items in the framework. Both are necessary, and U.S. experience suggests instances from other policy fields in which it was

---

[33] *See* Terrence K. Kelly, Ellen E. Tunstall, Thomas S. Szayna & Deanna Weber Prine, *Stabilization and Reconstruction Staffing: Developing U.S. Civilian Personnel Capabilities*, 2 RAND CORPORATION (2008), *available at* http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG580.pdf.

[34] *Id.*

[35] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE , GAO-12-365T, CONTINUED PROGRESS MADE IMPROVING AND INTEGRATING MANAGEMENT AREAS BUT MORE WORK REMAINS; TESTIMONY BEFORE THE COMMITTEE ON HOMELAND SECURITY, HOUSE OF REPRESENTATIVES, BY DAVID C. MAURER, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES (2012); U.S. GOV'T ACCOUNTABILITY OFFICE GAO-08-588, CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY, (2008).

necessary to combine organizations with resources and organizations with the technical skills necessary to achieve a goal. For example, in Iraq in 2003 and 2004, the U.S. focused on establishing competent police forces, which were thought to be the underpinnings of a stable society ("police primacy").[36] The task of establishing the Iraqi Ministry of Interior and police forces was given to professional police managers, most notably a former Commissioner of the New York City police force, a senior career DEA officer, and a Deputy Chief Constable from the U.K. However, after spending most of a year without making much progress, coalition military forces were given the policing task due to their ability to field far larger numbers of personnel and organize messy efforts in a conflict zone. The civilian police managers would continue providing technical expertise, but were no longer in charge.

Organizational capacity was deemed more important than superior technical competence in policing, but at the same time, the project retained technical capacity through the professional police managers. We may see a similar trend in cyber security, particularly if the U.S. is confronted with a major challenge that requires concerted response by an organization with both the fiscal and human resources needed for a nationwide response.[37] In the cyber field, the Department of Defense (DoD) has the obvious organizational advantage of combining fiscal and human resources with world-class technical capabilities.

As it happens, however, using DoD as the default "get the job done" organization to achieve cyber security goals runs counter to the intellectual basis of U.S. policy—namely, to rely principally on voluntary partnerships where in some real sense the private sector is an equal, non-compulsory, partner with (mostly non-DoD) Federal departments and agencies. There may also be issues that arise (particularly in using DoD as the default organization) where "who has the legal authority" and "who has the resources (and capacity)" are not aligned. Disaster response provides a good example of this

---

[36] Author's experience in the Office of National Security Affairs, Coalition Provisional Authority, 2004. The remainder of this example draws upon Kelly's personal observations.

[37] This is a potentially critical issue, especially if a crisis leads to DoD resources being used to support critical cyber infrastructures. In addition to the competing authorities for the use of military personnel in response to a cyber-initiated disaster cited above, an increased DoD role in domestic cyber security may raise other issues, such as *posse comitatus* if there is a law enforcement aspect to the operations they are involved with. *See generally* Susan W. Brenner & Leo. L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1015 (2010).

conflict. Federal troops have well-defined limitations on what they can do domestically within the United States that do not apply to the National Guard, yet federal troops also have far greater capabilities to bring manpower and material to bear on problems. In the aftermath of Hurricane Katrina, efforts to help the people of New Orleans were stymied due to these and similar structures on what federal troops could do.[38] Recognizing this, the DoD created mechanisms that would permit federal troops to work under the direction of National Guard commanders, permitting greater flexibility.[39]

IV. EXAMPLES OF GOVERNMENT POLICY WORKING

The four requisites for effective public policy are not a cookie cutter approach. We are reminded of those diagrams one sees in introductory public policy courses on "the policy process" that suggest that there is always some orderly process to follow. Goals, resources, authorities, and competency do not necessarily arrive packaged in neat boxes. What follows are two examples of successful government policy actions that illustrate this inherent messiness.

A. THE Y2K TRANSITION

The public-private partnership created to address the Y2K computer problem[40] was not the first such cyber partnership,[41] but it

---

[38] *See, e.g.*, *Lynn Davis et al., Hurricane Katrina: Lessons for Army Planning and Operations*, RAND CORPORATION (2007).

[39] NAT'L GUARD BUREAU, NATIONAL GUARD DOMESTIC LAW ENFORCEMENT SUPPORT AND MISSION ASSURANCE OPERATIONS 4–5 (2010), *available at* http://www.ngbpdc.ngb.army.mil/pubs/500/ngr500_5_angi10_208.pdf.

[40] The Y2K computer problem arose from software written that only used two digits for the year, e.g., 89 instead of 1989. Done to conserve memory at a time when computer memory was expensive, this convention caused some software to malfunction for dates involving years past 1999. *See, e.g.*, GAO, *Year 2000 Computing Challenges: Leadership and Partnerships Lead to Limited Disruption*, GAO/T-AIMD-00-70 (Jan. 27, 2000).

[41] Arguably the first public private partnership in what is now called cyberspace was the National Communications System, set up following the Cuban Missile Crisis to ensure that the largely private sector telecommunications providers would be able to support critical government needs during times of emergency. Telecommunications providers (private sector) and government agencies on the NCS work together through a variety of bodies under the NCS umbrella, notably the National Security Telecommunications Advisory Committee (providing private sector CEO level input to the NCS), the Network Security Information Exchange, and the NCS's National Coordinating Center which also serves as

remains one of the most significant and most significantly international of all. Led by the U.S. government, the effort to fix the Y2K problem was a truly collaborative effort between governments, governmental organizations, and the private sector. Yet, the effort had only the shell of a unitary structure and functioned more as a series of national agendas moving in sync.

Neither the U.S. nor any other government specified a standard for Y2K compliance.[42] Nations took action along two lines. One of these was sharing information and raising awareness. In the U.S., a special advisor to the President, John Koskinen, worked with industry and international bodies to encourage awareness and action in advance of the new millennium.[43] Koskinen's leadership role was essential to the partnership's success. He was highly successful and admired, with careers in government service and the private sector. Furthermore, it was obvious to the world that Koskinen had the very real support of the President. Through Koskinen's efforts, a series of international global and regional Y2K preparedness meetings were held with increasing participation and engagement as the year 2000 approached.[44] The International Y2K Cooperation Center was funded by the World Bank with contributions from the United States.[45] The banking and financial sectors were also very much engaged in Y2K preparations. The Joint Year 2000 Council functioned under the Bank for International Settlements in Basel, bringing together banking,

---

the ISAC for the telecommunications sector. *See Background and History of the NCS,* NAT'L COMM. SYS., http://www.ncs.gov/about.html (last visited Apr. 7, 2012).

[42] *See supra* note 40. TheY2K problem was that dates in databases prior to the year 2000 were typically represented with only to numbers to signify years. Programs that used these dates to do calculation would, therefore, mistake dates in the early 21st century as coming before dates in most of the 20th century, e.g., 00 (representing the year 2000) would be understood by these programs to fall before most dates in the 20th century, e.g., all dates from 1901-1999 (signified by "01" through "99"). Y2K compliance involved fixing databases so this problem would not happen.

[43] Frank James, *On the Record, John Koskinen*, CHI. TRIB. (Dec. 19, 1999), *available at* http://articles.chicagotribune.com/1999-12-19/news/9912190369_1_yale-law-school-alumnus-john-koskinen-y2k.

[44] For a list of several meetings, see *Year 2000 Activities*, WITSA, http://www.witsa.org/news/99feb.htm (last visited Apr. 7, 2012).

[45] INT'L Y2K COOPERATION CTR, http://www.iy2kcc.org (last visited Apr. 7, 2012).

market, and insurance regulators.[46] Over 200 major financial institutions around the world cooperated.[47]

The other major step that the United States (and Canada, in a slightly different format) took was creating incentives for private sector action. The U.S. Securities and Exchange Commission (SEC) required that public companies report on what, if anything, they were doing to prepare for Y2K.[48] The SEC left it up to investors and the market to determine whether a company was Y2K compliant or not and whether their actions were sufficient.[49] The SEC requirements are widely viewed as a being a power incentive for private sector action.[50] In Canada, there was widespread publicity and encouragement of investment to correct the problem. The existing Canada Corporations Business Act also imposed duties on directors, analogous to liability from environmental and computer virus cases.[51]

In the United States, the federal government also funded the creation of the Y2K Information Coordination Center (ICC), which, starting in late 1999, brought together in a single "war room" (actually two floors of a building near the White House) representatives from all the federal agencies, other levels of government, and major sectors of the economy.[52] Their objective was to monitor and, if necessary, coordinate responses to, any Y2K events at the time of the rollover.[53]

---

[46] Press Release, Bank for Int'l Settlements, Joint Year 2000 Council's Round Table Meeting Indicates Progress on Readiness and Contingency Planning in Financial Markets (July 1, 1999), *available at* http://www.bis.org/press/p990701.htm.

[47] *What Happened to Y2K? Koskinen Speaks Out*, THE CO-INTELLIGENCE INST. (Jan. 27, 2000), http://www.co-intelligence.org/y2k_KoskinenJan2000.html.

[48] *Id.*

[49] *Id.*

[50] Rep. James R. Langevin, Rep. Michael T. McCaul, Scott Charney, Lt. Gen. Harry Raduege & James A. Lewis, *Securing Cyberspace for the 44th Presidency*, CTR FOR STRATEGIC & INT'L STUDIES 51-52 (Dec. 2008), *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[51] 8 DALHOUSIE J. LEGAL STUD. 130, 145 (1999). As the article notes: "[E]nvironmental and computer virus case law ought to give directors and officers some indication of the standard of diligence and skill expected in the Y2K context." *Id.*

[52] Diane Frank & FCW Staff, *The Year 2000 Information Coordination Center Y2K Sentries*, CNN (July 20, 1999), http://articles.cnn.com/1999-07-20/tech/9907_20_sentries.y2k.idg_1_information-flow-fcw-agencies?_s=PM:TECH.

[53] *Id.*

Both of the authors worked at the ICC; it was a tangible instance of the government and the private sector working together to ensure cyber stability in the face of significant problems.[54]

The U.S. federal government spent about $8.5 billion on Y2K fixes (including about $20 million to build the ICC); worldwide spending on Y2K was estimated at about $200 billion, with the United States accounting in total for about $100 billion.[55]

In the end, there were few Y2K-related computer disruptions. This has led to criticism that Y2K computer problems were an imaginary crisis.[56] Koskinen certainly disagrees: "It was clear to me [in 1998] after talking with a lot of experts, if nobody did anything else beyond what they had already done up until [then] that the world as we knew it would end."[57]

Along with credible leadership and the backing of the President, real regulatory-based incentives for private sector action, and significant public (as well as private) dollars committed, one other factor helps to explain the success of the Y2K effort. Everyone "had a goal, which was to deal with Y2K. So there was a common enemy people could deal with."[58]

B. THE CLEAN AIR ACT

Another policy example that has a number of similarities to cyber security is the history of the Clean Air Act of 1970 and its substantial amendments in 1990.[59] After a long debate and juggling of competing

---

[54] One of us (Hunker) spent a number of hectic days from the end of December 1999 through January 2000 working with private sector software engineers staffing the ICC to understand better a new worm, "Stacheldracht" (German for barbed wire) which was feared—subsequently correctly, but later in 2000—to be capable of launching DDOS attacks.

[55] U.S. DEP'T OF COMMERCE, THE ECONOMICS OF Y2K AND THE IMPACT ON THE UNITED STATES (1999), *available at* *http://www.esa.doc.gov/sites/default/files/reports/documents/y2k_1.pdf.*

[56] *See Y2K Precautions Successful or Excessive,* CNN (Mar. 14, 2000), http://articles.cnn.com/2000-01-02/us/y2k.hyped_1_programming-flaw-price-tag-glitches?_s=PM:US.

[57] *What Happened to Y2K?, supra* note 47.

[58] *Id.*

[59] *See generally, Summary of the Clean Air Act*, U.S. ENVIRONMENTAL PROTECTION AGENCY, http://www.epa.gov/regulations/laws/caa.html (last visited Apr. 7, 2012).

interests and constituencies, (e.g., environmentalists versus those concerned about losing jobs in industries such as coal and automobile manufacturing) the Clean Air Act of 1970 was passed, but it proved largely ineffective. Part of the problem was that the issue was not well-defined, due to the constant discovery of new technologies and debates on what pollutants needed to be controlled, what levels were acceptable, and what the economic costs of regulation would be.[60] In other words, the problem was not adequately defined among the key stakeholders and its solution was not effective because competing interest groups could not agree on first order issues. Furthermore, the Clean Air Act of 1970 did not give the U.S. federal government significant enforcement powers; these were relegated to lower levels of government. Although the Act provided guidelines that governed pollution, the Environmental Protection Agency did not have the mandate, resources, or organization to enforce them. Furthermore, several government agencies shared policy oversight of areas covered by the 1970 Clean Air Act (e.g., EPA, the Department of the Interior, and the Nuclear Regulatory Commission), so lines of responsibility were not clear. Similarly, oversight in Congress was split between many committees.[61] In short, air pollution policy under the Clean Air Act of 1970 had many of the characteristics of the first generation of cyber security policies created under President Clinton. These included:

- Difficulty articulating a policy that would be acceptable to all constituencies and help solve the problem;
- Inadequate authorities to enforce the policy once it was adopted;
- Limited resources to do so; and
- Limited organizational ability to create and enforce the implementing regulations.

---

[60] *See, e.g.*, Robert M. Friedman, Jana Milford, Richard Rapoport, Nancy Szabo, Kathryn Harrison & Sally Van Aller, *Urban Ozone and the Clean Air Act: Problems and Proposal for Change*, THE FEDERATION OF AM. SCIENTISTS: OFFICE OF TECH. ASSESSMENT ARCHIVE 1 (Apr. 1988), *available at* http://www.fas.org/ota/reports/8841.pdf.

[61] *See generally, Summary of the Clean Air Act*, U.S. ENVIRONMENTAL PROTECTION AGENCY, http://www.epa.gov/regulations/laws/caa.html (last visited Apr. 7, 2012).

However, in this case, the government demonstrated that (with two decades' further work) it could adapt its environmental policies. Most of the shortcomings of the 1970 Clean Air Act and its implementing arrangements were addressed in the Clean Air Act Amendments of 1990, which also provided for measures to alleviate the 1970 Act's negative economic effects (e.g., stipends and training for coal miners put out of work by regulations that limited the economic value of high-sulfur coal stipulations that permitted the buying and selling of pollutant quotas). [62] The result has been a set of policies, embodied in laws and regulations, that evidentially are acceptable to most major constituencies, are implementable and enforceable, have manageable economic effect on the country, and produce a vast improvement in air quality.

To summarize, the four factors that shape how well the federal government is positioned to achieve its stated policy, (1) clear goals, (2) supporting authorities, (3) adequate resources, and (4) the capabilities, capacity, and relationships within and beyond the government to succeed, were fulfilled by the 1990 amendments to the Clean Air Act.

V. CREATING EFFECTIVE CYBER SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION POLICY

We have already discussed why, under the best of circumstances, effective cyber security policy is difficult to construct and execute. These difficulties rest largely in factors inherent to the technology and the foundations of the Internet. In spite of these challenges, there are aspects where it seems that the government has had some success (e.g., in the definition of the problem, the identification of solutions that require research and development, or the protection of national security systems).

In the most critical facets of cyber security policy, particularly those involving the private sector, our view is much more pessimistic. In private sector-related cyber security policy, there is a fundamental mismatch between articulated goals and the authorities, resources, and capabilities of the government to meet them. But this mismatch is not uniform. Cyber security policy is far too multifaceted for that. Indeed, in some instances, even for goals directed towards the private

---

[62] *See generally, Overview–The Clean Air Act Amendments of 1990*, U.S. ENVIRONMENTAL PROTECTION AGENCY, http://www.epa.gov/oar/caa/caaa_overview.html (last visited Apr. 7, 2012).

sector, we observe some success. But these areas of "four-factor alignment" are relatively few. It is more common that government has policy goals that it simply does not have the capabilities to achieve.

The basic reasons for the fundamental misalignment between government policy ambitions and its public-private sector cyber security capacity are simple: Cyber security policy requires policy engagement in a broad swath of the economy. Indeed, one is challenged to think of other policy initiatives with so broad a sweep. Also, it rests on the secure performance of the Internet and other global networks. However, this broad swath of policy reach is at odds with the realities of government. Stated differently, even if we look only at those economic and government sectors central to cyber security policies, there are really only a few areas of particular interest and concern for the government. These include the cyber efforts by the defense and intelligence communities that are clearly primarily the government's domain, those focused at protecting the information infrastructure upon which critical infrastructures and therefore the health, welfare, and safety of Americans depend, and standard setting and related issues that have a direct bearing on how the information infrastructure functions.

Yet, if we look further at what regulatory and other authorities and resources the government has, even in areas of concern such as critical infrastructure, there are only a few sectors in which the government is truly operationally engaged with the infrastructure. For example, federal regulation in the finance sector provides some leverage and relations with the financial sector that can be used to enhance cyber security, yet the federal government has almost no regulations or relationships with the chemical sector that could provide similar results.[63] In some cases, government agencies do not have the

---

[63] No single federal agency has exclusive jurisdiction over the banking and financial sector. For example, the Office of Thrift Supervision, part of the US Treasury Department, audits and inspects savings and loan banks to check compliance with government regulations and policies so as to ensure the safety and soundness of deposits in thrift banks. The Securities and Exchange Commission (SEC) regulates many securities markets (but not all, including commodity markets) on a continuous basis, receives regular reports of the financial status of companies traded publicly, and, in general, promotes full public disclosure of accurate information needed by investors, protecting the investing public against fraudulent and manipulative practices in financial markets. Another major federal agency (though independent of direct control by the U.S. Government) is the Federal Reserve System (the 'Fed'). The Fed sets US monetary policy, regulates (as needed in cooperation with other regulatory agencies) the health of U.S. banks and financial service institutions, and maintains the stability of the financial system (a role made prominent by the Fed's role in the recent 'subprime' financial crisis). These responsibilities require a continuous engagement with U.S. and multinational hanks and financial institutions, and the sort of detailed market and institutional knowledge that allows the Fed (and the U.S. Treasury) to

technical competencies to understand how certain actions will affect a particular sector. In terms of securing much of cyberspace, the government's reach exceeds its grasp.

This short explanation is, of course, too simplified to offer insight into the particulars of a complex policy endeavor, yet there are three overlapping themes that shape this landscape of "creeping failure."

A. THEME ONE: FUNDAMENTAL UNRESOLVED ISSUES OF GOVERNANCE VERSUS TECHNICAL CAPACITY

A major challenge for the United States is developing consensus for the areas over which the government needs to be able to exercise control with respect to cyber security, and what part of government will do that. Here, we focus on which unit of government has the authorities, resources, and capabilities to exercise governance in important cyber security areas. Critical functions for cyber security include the capacity to monitor and generate intelligence on threats and effective deterrence against would-be bad actors, particularly those that are state-sponsored. We note here instances in which national policy has created an inherent mismatch between capabilities and authorities.

The U.S. Computer Emergency Response Team (US-CERT) is the U.S. government's lead organization for information sharing and monitoring, detecting, and mitigating the effects of attacks.[64] On the civilian side of government, it can provide some level of situational awareness of threats, but has almost no ability to anticipate or deter threats.[65] Many organizations do some formal and informal

---

be active players in complex financial markets. Nothing remotely similar to these federal capacities exists for the chemical industry.

[64] *About Us,* US-CERT, http://www.us-cert.gov/aboutus.html (last visited Apr. 7, 2012).

[65] 'CERT' stands for Computer Emergency Readiness (or "Response") Team. What is sometimes erroneously referred to as "the CERT" is not a single organization. The CERT Coordination Center (CERT/CC) is part of the Software Engineering Institute at Carnegie Mellon University. The CERT/CC was established in December, 1988, following the first automated network security incident, the "Morris worm," which brought much of the Internet to a halt. Following this incident, the Defense Advanced Research Projects Agency (DARPA) funded the CERT Coordination Center to give security experts a central point for coordinating responses to security incidents and to help in their prevention. DARPA also charged the newly formed center with serving as a central point for identifying and correcting vulnerabilities in computer systems, conducting research to improve security, keeping close ties with the relevant research activities of others, and initiating proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

information-sharing. The US-CERT is supposed to be at the center of this sharing. In fact, the US-CERT may be best thought of as a national "help desk." In October 2009, in order to provide a central

---

From the start, it was clear that a single group could not accomplish the necessary work: the CERT/CC thus became one of the founding members of the Forum of Incident Response Teams (FIRST), a cooperative network of independent computer security incident response teams (CSIRTs) in the U.S. and abroad. The CERT/CC also helps organizations to form CSIRTs and provides guidance and training to both new and existing teams, especially those with nation-level responsibility.

The US –CERT is a different organization, created in 2003 as one of the initiatives of the *National Strategy to Secure Cyberspace*. *See* THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf. That strategy directed as follows:

> DHS will create a single point-of-contact for the federal government's interaction with industry and other partners for 24 x7 functions, including cyberspace analysis, warning, information sharing, major incident response, and national-level recovery efforts. Private sector organizations, which have major contributions for those functions, are encouraged to coordinate activities, as permitted by law, in order to provide a synoptic view of the health of cyberspace on a 24 x 7 basis.

Id. at 22. US-CERT is now the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). US-CERT is independent of other groups using "CERT" in their titles, although the US-CERT coordinates as needed with them on security incidents. US-CERT continues to draw on CERT/CC capabilities to help prevent cyber attacks, protect systems, and respond to the effects of cyber attacks across the internet.

A host of other countries now have CERTs or CERT-like organizations as well, including many European nations, India, Pakistan, Argentina, Brazil, and Chile. The setups vary: Germany has multiple CERTs, while France has one operated as a non-profit center by major industries, and another run by the government. The cooperative network of independent CSIRTs around the world all more or less follow the U.S. operating model as their core function, whereby private and public entities can report major cyber incidents or vulnerabilities to the appropriate regional CERT, which may then help out in any number of ways, from analyzing threats and disseminating alerts to helping defend against an attack in progress.

Reflecting increasingly sophisticated challenges, the larger CERT program has expanded to include education and training, research and development, situational awareness, forensics, and organizational security, including work in organizational resilience and insider threat. The CERT Program is also concentrating on threats that affect national and economic security, with a focus on government and critical infrastructure. The CERTs are routinely valuable and have had some spotlight moments; for instance, global CERTs worked with the Estonia CERT to deal with the DDOS attacks on that country in 2007. A major limitation is that many incidents are not reported to CERTs. Indeed, if all were, the CERTs would probably be hard pressed to process them.

place for various federal and private sector organizations to coordinate efforts to address cyber threats and respond to cyber attacks, the Department of Homeland Security (DHS) developed an integration center known as the National Cybersecurity and Communications Integration Center, which is composed of the US-CERT and the National Coordinating Center for Telecommunications.[66]

The system based on the US-CERT is widely criticized. Only a small fraction of private sector partnership members surveyed by the GAO in 2010 felt that the government was being effective in providing timely and actionable cyber threat information (27%), timely and actionable cyber alerts (27%), access to actionable classified or sensitive information, such as intelligence and law enforcement information (16%), or a secure information-sharing mechanism (21%).[67]

According to DHS officials, US-CERT's ability to provide information is affected, among other things, by restrictions that do not allow individualized treatment for any one private sector entity as opposed to any other private sector entity, making it difficult to formally share specific information with entities that are being directly affected by a cyber threat.[68] In addition, because US-CERT serves as the nation's cyber analysis and warning center, there is a premium set on ensuring that its warnings are accurate. Therefore, US-CERT's products are subjected to a stringent review and revision process that can adversely affect the timeliness of those products, potentially adding days to the release if classified or law enforcement information must be removed from the product.[69]

---

[66] *About the Communications Integration Center*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm (last visited Apr. 7, 2012); *see also* GOV'T ACCOUNTABILITY OFFICE, GAO 10-628, CRITICAL INFRASTRUCTURE PROTECTION: KEY PRIVATE AND PUBLIC CYBER EXPECTATIONS NEED TO BE CONSISTENTLY ADDRESSED 19 (2010) [hereinafter GAO, CRITICAL INFRASTRUCTURE PROTECTION].

[67] *Id.* at 16.

[68] *Id.* at 17. ("Federal partners are not meeting private sector stakeholders' expectations, in part, because of restrictions on the type of information that can be shared with the private sector. According to DHS officials, US-CERT's ability to provide information is impacted by restrictions that do not allow individualized treatment of one private sector entity over another private sector entity—making it difficult to formally share specific information with entities that are being directly impacted by a cyber threat.").

[69] *Id.* at 17.

Private sector officials and cyber experts stated that having a single or centralized government source for cyber-related information is important to (1) avoid confusion about who is the authoritative source, (2) have a consistent message communicated, and (3) coordinate a national response.[70] The Government Accountability Office (GAO), having convened a panel of cyber security experts, concluded that creating an accountable, operational cyber security organization would be essential to improving our national cyber security posture.[71] According to this analysis, there needs to be an independent cyber security organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, the military, the intelligence community, and the nation's international allies to address incidents against the nation's critical cyber systems and functions.[72]

There is, arguably, only one agency of the U.S. government that can provide this level of coordination to produce threat forecasts and warnings: U.S. Cyber Command in the DoD.[73] This command incorporates capabilities of the National Security Agency, the world's foremost military high-tech spying agency, and an operational command.[74] As a major command, it provides significant capabilities to engage in "command and control," in addition to the world-class cyber capabilities noted above.[75] This includes the ability to manage and coordinate among many entities. There is a strong argument that this role should not be performed by the military, but recreating these capabilities in a civilian agency of government would take many years and billions of dollars.

---

[70] *Id.* at 15.

[71] GOV'T ACCOUNTABILITY OFFICE, GAO 09-432T: KEY IMPROVEMENTS ARE NEEDED TO STRENGTHEN THE NATION'S POSTURE 7–12 (2009), *available at* http://www.gao.gov/new.items/d09432t.pdf.

[72] *Id.*

[73] *See* Press Release, U.S. Dep't of Defense, DOD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander (May 21, 2010), *available at* http://www.defense.gov/releases/release.aspx?releaseid=13551.

[74] U.S. DEP'T OF DEFENSE, CYBER COMMAND FACT SHEET (2010), *available at* http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYBERCOM%20Fact%20Sheet%20to%20replace%20online%20version%20on%20OCT%2013.pdf.

[75] *Id.*

A very real potential exists for conflict or confusion between needed or desirable capabilities and existing legal restrictions. It is very likely that Cyber Command will play an increasingly important role in cyber security, particularly since we now seem to have crossed a threshold of state-sponsored cyber attacks that go beyond espionage to actually damaging infrastructure.[76] A much more significant DoD role may be driven by operational needs, despite real concerns about privacy and the proper role of the military in society. Even if we accept that Cyber Command has the technical cyber tools to address the most important Internet security problems, the other challenges to effective government engagement highlighted above would remain unaddressed.

B. THEME TWO: A PROFOUND MISMATCH BETWEEN WHAT GOVERNMENT CAN DO AND WHAT IS EXPECTED OF PUBLIC-PRIVATE PARTNERSHIPS

Defending critical infrastructure from cyber attacks is a core element of U.S. cyber security policy. Because most critical infrastructures are owned and operated by the private sector, the four prerequisites for good public policy articulated above are very difficult to meet. This challenge severely limits the effectiveness of government action toward this core goal.

Securing cyberspace requires government and the private sector to work together. The private sector owns, designs, deploys, and maintains much of the nation's critical infrastructure, much of which depends on the Internet or other cyber-infrastructure to operate.[77] This dependence is important because, unlike certain other elements of national security, the government cannot secure cyberspace alone. In particular, government has a core interest in defending the nation, and in pursuit of this interest it defined a set of critical infrastructures in cooperation with the private sector.[78] As part of its mandate to

---

[76] *See, e.g.*, the discussion about Stuxnet, *supra* Part I.

[77] CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 66, at 1 (Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in eighteen sectors: "agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.").

[78] *Id.*

protect the nation from a crippling attack, it must protect these infrastructures. As a result, there is a divergence between cyber security responsibility, because the government must protect the nation from crippling attacks, and cybersecurity control, because the government does not manage the assets or provide the function that must be protected.[79]

These combined efforts of government and the private sector are loosely described as public-private partnerships; loosely, because the public and private elements of public-private partnerships have different, often ill-defined, and contrary goals and take on a variety of different forms. For example, government may want to regulate elements of cyber space, whereas the private sector does not like regulation as it costs them money to meet mandates and decreases their flexibility, or the public may object to the government limiting freedoms online. The recent defeat of the House of Representatives' effort to protect intellectual property online (the Stop Online Piracy Act, or SOPA) and the Senate's similar efforts (the Protect IP Act, or PIPA) is a recent example of this latter conflict.[80] Despite this variety, however, there is a common structure for the interface between government and industry. Most formally, there are Sector Coordinating Councils organized under the auspices of the Department of Homeland Security, which represent the various officially designated critical infrastructure sectors in developing and coordinating plans and actions with their respective federal agencies or departments, called Sector Lead Agencies.[81] In addition to these

---

[79] *Securing Cyberspace for the 44th Presidency*, *supra* note 50 at 43.

[80] One example of the attacks on SOPA and PIPA is Lifehacker.com's article, *All About PIPA and SOPA, the Bills That Want to Censor Your Internet*, which is available at http://lifehacker.com/5860205/all-about-sopa-the-bill-thats-going-to-cripple-your-internet.

[81] The National Infrastructure Protection Plan (DHS, 2006) relies on a sector partnership model as the primary means of coordinating government and private sector CIP efforts. Under this model, each sector has both a government council and a private sector council to address sector-specific planning and coordination. The government and private sector councils are to work in tandem to create the context, framework, and support for coordination and information-sharing activities required to implement and sustain that sector's CIP efforts. The council framework allows for the involvement of representatives from all levels of government and the private sector, so that collaboration and information-sharing can occur to assess events accurately, formulate risk-assessments, and determine appropriate protective measures. Information-sharing also takes place under Information Sharing and Analysis Centers (ISACs) which were formed under earlier versions of U.S. cyber security policy and have been incorporated into the sector partnership model. GOV'T ACCOUNTABILITY OFFICE, GAO-07-39, CRITICAL INFRASTRUCTURE PROTECTION: PROGRESS

sector specific partnerships, a number of other initiatives are under way which require the cooperation of the private sector with the federal government (e.g., work to promote network standards). For example, the Federal National Institute of Standards and Technology (NIST) Standards Coordination Office works with industry to set standards in diverse sectors including cyber security, electric power grids, health IT systems, and emergency communication interoperability.[82]

Whatever their particular form, public-private partnerships share a common mission; they serve as identifiable instruments, whether formally organized or not, by which the government has sought to promote national security without resorting to regulation or mandates.

The public-private model has never resolved its fundamental dilemma: private companies have different incentives and responsibilities than government. In the simplifying assumptions of the field of economics, companies seek to maximize profits. Most major companies today have limited, and fading, national identity. Spending money on U.S. security is not necessarily a primary concern, and in some cases may be viewed as in conflict with the fiduciary responsibility corporate officers have to their stockholders. Similarly, security measures that cause a corporation to be less competitive than others in a sector directly affects a firm's willingness to take on additional security measures.

The logic underlying public-private partnerships includes the government's assumption that infrastructure owners will "do the right thing" with respect to cyber security as it applies to critical infrastructure protection. However, in the face of uncertain threats, there is no common understanding of what "the right thing" is. Even if private companies agreed with the government that certain actions to protect cyber security are important, they would not follow through if the initiative will put them at a fundamental disadvantage with their competitors or cause stockholders to demand changes in company leadership. Unfortunately, this assumption about doing "the right

---

COORDINATING GOVERNMENT AND PRIVATE SECTOR EFFORTS VARIES BY SECTOR CHARACTERISTICS 3 (2006).

[82] NIST STANDARDS COORDINATION OFFICE, NATIONAL SCIENCE AND TECH. COUNCIL'S SUBCOMMITTEE ON STANDARDS REQUEST-FOR-INFORMATION, ISSUED DECEMBER 2010: EFFECTIVENESS OF FEDERAL AGENCY PARTICIPATION IN STANDARDIZATION IN SELECT TECHNOLOGY SECTORS (2010), *available at* http://standards.gov/upload/RFI-Summary-5-13-final2-2.pdf.

thing," and therefore the underlying logic of public-private partnerships, is deeply flawed.

Furthermore, U.S. cyber security and critical infrastructure protection do not pose a simple national issue in all cases. Some infrastructures are international. The governments of many other countries are far less accommodating than our own when seeking to protect national security interests that are in private sector hands. For instance, in April 2011, the UAE threatened to ban individuals and small businesses from using encrypted BlackBerry settings for email, web browsing, and BlackBerry Messenger as part of security fears sweeping the Middle East.[83] Authorities in India, Saudi Arabia, Indonesia and Lebanon share these "state security" concerns as well, as all have been pushing for greater access to data transmitted between BlackBerry devices.[84] So, putting aside the hope that the private sector will "do the right thing," why might some public-private partnerships work?

A core theme is that public-private partnerships work in some cases and not in others, and that most partnerships do not meet the test of effectiveness. This is largely because private entities do not have the incentives to do what government wants of them. Public-private partnerships can succeed in some cases, but their success depends on unique factors and circumstances not shared by every sector or situation.[85] We can point to significant variations, sector by sector, in the fundamentals of both how government can exercise influence and how various parts of the private sector are organized to explain our conclusions. Simply put, in many cases, the government simply does not have the authorities and adequate resources to provide the right incentives to shape the decisions of private owners of critical infrastructure that are required for public-private partnerships to succeed—incentives that would cause private sector partners to perceive that it is in their self-interest to assume some of the national security obligations that historically have been the sole province of the state.

---

[83] Josh Halliday, *UAE to Tighten BlackBerry Restrictions*, THE GUARDIAN (Apr. 18, 2011), http://www.guardian.co.uk/technology/2011/apr/18/uae-blackberry-emails-secure.

[84] *Id.*

[85] These issues are explored in much greater detail on a sector specific basis in two related papers: Jeffrey Hunker, *Global Leadership in Cybersecurity: can the U.S. Provide It?*, *available at* http://moritzlaw.osu.edu/students/groups/is/files/2012/05/Hunker.pdf (last visited May 16, 2012) and Mark MacCarthy, *Government and Private Sector Roles in Providing Information Security in the U.S. Financial Services Industry, 8* ISJLP 242 (2012).

Other recent commentaries on public-private partnership have also concluded that incentives or regulations coming from the government are needed to make public-private partnerships work.[86] As *Securing Cyberspace for the 44th Presidency* notes:

> In pursuing the laudable goal of avoiding overregulation, the [National Strategy to Secure Cyberspace] essentially abandoned cyber defense to ad hoc market forces. We believe it is time to change this. In no other area of national security do we depend on private, voluntary efforts. Companies have little incentive to spend on national defense as they bear all of the cost but do not reap all of the return...We believe that cyberspace cannot be secured without regulation.[87]

We conclude that it is risky to use public-private partnerships in their current incarnation as a generalized policy instrument. This conclusion leads us to a key question: what if public-private partnerships are not an effective approach for addressing cyber-driven national security threats to infrastructures that are mostly in private hands? This question is important, given the degree to which government relies on public-private partnerships and the significant challenges government faces in achieving its goals through more direct public policy means. Given the increasing likelihood that state or non-state actors will be using disruptive cyber attacks as a means of expressing power, governments, in one way or another, will have to confront this issue of effectiveness.

C. THEME THREE: U.S. POLICY WILL NOT "SOLVE" CYBER SECURITY

Some problems must be managed rather than solved, especially if the authorities and resources necessary to solve them are not provided, or they are too ill-defined or complex for reasonable solutions. The conflicts in Iraq and Afghanistan are good examples of such circumstances. In Afghanistan, in particular, real solutions require the convergence of political, social, economic and security

---

[86] *See, e.g., Addressing Cyber Security Through Public-Private Partnerships: An Analysis of Existing Models*, INTELLIGENCE AND NATIONAL SECURITY ALLIANCE (Nov. 2009), *available at* http://www.insaonline.org/assets/files/CyberPaperNov09R3.pdf.; *Securing Cyberspace*, *supra* note 50, at 50–51.

[87] *Id.*

efforts that seem extremely unlikely. Coalition forces have significant capabilities in the security domain, but very limited capabilities to affect the other domains. These lopsided capabilities present a set of problems that cannot be solved in any comprehensive manner. Yet, while we cannot decisively win the conflict there, the Afghan government will not lose so long as coalition forces remain. This provides space to manage a messy set of problems, hopefully in a positive direction.

In Iraq in 2007, General David Petraeus and Ambassador Ryan Crocker recognized that progress, rather than comprehensive solutions, should be the goal.[88] As a result, they agreed to efforts that, if viewed in isolation, would appear less than perfect (e.g., arming Sunni groups that months earlier were fighting against U.S. forces). In the context of Iraq in 2007, these steps helped move closer to achieving U.S. objectives in Iraq.

These examples provide insights into how to think about many aspects of cyber security. Policy solutions that seek to decisively solve the cyber security challenge are likely to lead to disappointment, whereas efforts that identify acceptable conditions, help build consensus on what must be done, and try to manage the problem in a positive direction (whatever that is) are more likely to demonstrate progress.

This lesson seems to apply—in spades—to issues surrounding the global functionality of the Internet. As it stands, the U.S. government and U.S. cyber security policy have only limited and very indirect influence over the standards[89] and functionality of the global Internet. Certainly, the structure of public-private partnerships has only a limited role.[90] As defined for the NIPP public-private partnerships, the IT sector "[p]roduces information technology and includes hardware manufacturers, software developers and service providers, *as well as the Internet as a key resource.*"[91] A prime objective of the national

---

[88] One of the authors, Kelly, served as Embassy Baghdad's Director of Policy, Planning and Analysis from February 2006 through April 2007. These are his observations.

[89] Officially, the Internet does not have "standards" but instead operates through a consensus system.

[90] *See* discussion *supra* Part I.

[91] Thompson & Jackson-Lee, *supra* note 23, at 7. The communications sector "provides wired, wireless, and satellite communications to meet the needs of businesses and governments." *Id.* In other words, the communications sector is responsible for the Internet backbone and pipes, but not for its functioning. The NIPP definition, by contrast, seems nonsensical: "Information Technology (IT) critical functions are sets of processes

cyber security agenda is to ensure a secure and reliable Internet.[92] According to the partnership structure, that objective is the function of the IT sector partnership. In that role, the IT partnership is, if not failing, certainly not succeeding. Here, we can look instructively at the case study of the transition to IPv6.

The Internet runs on a set of protocols, TCP, or Transport Control Protocol, and IP, or Internet Protocol. The IP determines the characteristics of Internet data packets, including their size and addressing. Most of the Internet now runs on IP version 4 (IPv4).[93] Yet, under IPv4 (barring some sneaky "workarounds"), the Internet can support only about four billion connected devices.[94] This address space has already run out though the consequences will take some time to be felt by most users and would-be users. IPv6 is needed because it provides space for many more connected devices. IPv6 also provides for a number of other desirable features, including much better security and quality of service.[95]

Transitioning from IPv4 to IPv6 is challenging. IPv6 is not backward compatible with IPv4, because they are completely different protocols and do not interact. Hence, "[t]he problem is that the *first* person [on the Internet] who wants to turn off IPv4 has to wait for the *last* person to add IPv6."[96] Also, IPv6 presents no discernible advantages to most individual users, although collectively everyone would benefit. The transition to IPv6 while maintaining IPv4 capabilities will not be painless, and will involve some work and sophistication on the part of systems administrators. Though IPv6 was standardized worldwide in 1995, IPv6 penetration as of January 2012

---

that produce, provide, and maintain products and services. IT critical functions encompass the full set of processes (e.g., R&D, manufacturing, distribution, upgrades, and maintenance) involved in transferring supply inputs into IT products and services.") *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, U. S. DEP'T OF HOMELAND SECURITY 12 (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[92] *Id.*

[93] *See* discussion *supra* Part I.

[94] Tweney, *supra* note 12.

[95] SILVANO GAI, INTERNETWORKING IPV6 WITH CISCO ROUTERS 153-64 (2007), *available at* http://www.ip6.com/us/book/Chap8.pdf.

[96] Iljitsch van Beijnum, *There Is No Plan B: Why the IPv4-to-IPv6 Transition Will Be Ugly*, ARS TECHNICA (Sept. 29, 2010), http://arstechnica.com/business/news/2010/09/there-is-no-plan-b-why-the-ipv4-to-ipv6-transition-will-be-ugly.ars/2

was about 0.4%.[97] From a cyber security perspective, this failure to transition is bad for at least two reasons. First, the Internet is, in a sense, headed for a brick wall. Addresses have run out, but few ISPs have put in place IPv6, which will be required for any reasonable expansion of the Internet.[98] Second, IPv6 has significantly improved security and reliability characteristics over IPv4.[99] The Internet will be, at least marginally, more secure after the transition.

The question for this effort is, who has the responsibility, within the U.S. public-private partnership model, for advancing such an important agenda as IPv6 implementation? The answer is, apparently, no one. This represents a real failure of the public-private partnership model. The transition to IPv6, which would contribute to the security of the Internet, is not part of the public-private partnership agenda. The National Plan says that the U.S. government "must understand the merits of, and obstacles to, moving to IPv6 and, based on that understanding, identify a process for moving to an IPv6 based infrastructure."[100] Since then, the federal government has subsequently adopted a plan for IPv6 transition that makes no reference to the private sector.[101] Neither the IT Sector Coordinating Committee nor the IT-ISAC appears to have any significant involvement in this issue.

Admittedly, the transition from one global Internet protocol to another is challenging, and the lack of any effective "governance" of the Internet makes this transition even more daunting. "Internet governance" is in most ways an oxymoron. The Internet Engineering Task Force (IETF) is a loosely organized international Internet

---

[97] *IPv6 Statistics*, GOOGLE (Jan. 6, 2012), http://www.google.com/intl/en/ipv6/statistics (approximately 0.38% of users would access Google over IPv6 if Google had an IPv6 address as of January 6, 2012)

[98] *See infra* note 101.

[99] Samuel Sotillo, *IPv6 Security Issues*, http://www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf (last visited Apr. 7, 2012).

[100] U.S. COMPUTER EMERGENCY READINESS TEAM, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 30 (2003), *available at* http://*www.us-cert.gov/reading_room/cyberspace_strategy.pdf.*

[101] gogo6videos, *gogoNET LIVE! IPv6 Conference: USGv6: US Government IPv6 Transition Activities by Dale Geesey*, YOUTUBE (Jan. 13, 2011), http://www.youtube.com/watch?v=U50qLoKQlCk; Dale Geesey, *USGV6: US Government IPv6 Transition Activities*, GOGONET (Nov. 4, 2010), http://*gogonetlive.com/4105/pdf/gogoNET_LIVE/Dale_Geesey.pdf.*

standards body.[102] The IETF, through a consensus process, develops Requests for Comments (RFCs) that, after a vetting, become the closest thing that the Internet has for technical standards. The adoption of RFCs is, however, a voluntary process. ICANN, which is frequently, but mistakenly, referred to as governing the Internet, is concerned only with issues of domain name allocation.[103] The public-private model here has simply left this important global issue off of the agenda. Governments worldwide have not defined a way ahead. This absence of a multinational agenda for what is patently a global network is, in our view, a major failing of the existing public-private model, and more generally of Internet governance, and hence cyber security. In this domain, in particular, the four factors for effective public policy would have to work on an international level. Given the fact that it is too difficult in most cyber security domains to do this on a national level, it is no surprise that little progress has been made here.

V. CYBER POLICY IN CRITICAL INFRASTRUCTURE PROTECTION: WHAT NEXT?

Cyber policy in critical infrastructure protection does not rest on a firm basis with respect to its ability to address all-important risk factors, or the prerequisites to develop and enforce effective policy. In particular, government does not own or closely regulate most critical infrastructures, nor does it have the authority to cause the infrastructure owners and operators to address cyber security problems. Government has also not been able to create effective incentive systems to cause owners and operators to adequately address cyber security. In part because government lacks key authorities and in part because responsibility for cyber security cuts across dozens of federal departments and agencies, human and fiscal resources are also inadequate to the task of protecting critical infrastructures. Finally, while public-private partnerships and the organizational structures created to make them work have been at best a mixed success, it is evident that the government has neither the internal organization nor the relationships among its own agencies and with the private sector for success.

---

[102] THE INTERNET ENGINEERING TASK FORCE, http://www.ietf.org (last visited Apr. 7, 2012).

[103] INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org (last visited Apr. 7, 2012).

What is a reasonable way ahead? How can we fulfill the four factors for effective public policy, which include the need for consensus on the problem and how to solve it? If we do nothing, then most likely the DoD will be ordered to step in when there is a crisis. If the crisis is severe enough, it could lead to the DoD being given this charge on a permanent basis. Yet, as noted above, there are real philosophical and perhaps legal objections to this default position, and the DoD does not, and should not, have deep knowledge about how the private sector operates. In that sense, the DoD is an inappropriate department to have this responsibility, yet the other obvious alternatives are also distasteful in their own way. They might include:

- Regulation that would provide government with the tools to create incentives needed to make public-private partnerships more effective, but would also come with economic costs; or

- More money (i.e., more federal resources to create capabilities similar to those of Cyber Command in the civilian side of government) or subsidies to provide incentives for the owners of critical infrastructures or possibly both.[104]

We will not pretend that we have the agenda for cyber security and critical infrastructure protection. As noted above, the problems are too complex and the solutions elusive. However, if one looks to the Y2K crisis as a guide for what actions are possible, one cannot escape the need for public leadership and some public resources for direct requirements and incentives for private sector action.

VI. CONCLUSION

[104] Others have argued that DHS, and not DoD, must have the principle role in the public-private partnership. *See* Gregory T. Nojeim, *Cybersecurity: Ideas Whose Time Has Not Come–And Shouldn't*, 8 ISJLP 408 (2012). We simply point out that this will require substantial funding increases for DHS to create capacity analogous to that of the NSA. The argument for subsidies to the private sector is the obverse of the argument for private sector regulation: both are based on the recognition that market forces alone are sufficient to incentivize the private sector collectively to meet national security needs. In other words, there is a gap between what the private sector voluntarily provides, and what the Nation requires. *See also Securing Cyberspace for the 44th Presidency*, *supra* note 50, at 50–54.

Developing and implementing sound cyber security policy is very difficult. Our conclusion, echoed in many of the subsequent articles in this issue, is that we are, if not failing, then not succeeding in this policy making task. Collectively, however, we believe that as a community of researchers, practitioners, and policy makers, it is our responsibility to look beyond comfortable platitudes and examine what it is that works, and does not – and also why. Our discussion in this introductory Article is intended to set the theme, if not the specifics, for the balance of this Issue, placing cyber security in its proper context as a problem of public policy – and thus, ultimately, for democratic decision making.