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

Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?

PAUL ROSENZWEIG*

I. INTRODUCTION

"Laws, like sausages, cease to inspire respect in proportion as we know how they are made." This famous quote is often attributed to Germany's Iron Chancellor, Otto von Bismarck. Like so many things that everyone "knows" to be true, the attribution is wrong; the words were first written by John Godfrey Saxe, an American lawyer-poet.[1]

This short tale therefore serves a two-fold purpose as the epigrammatic opening for a discussion of the cybersecurity policymaking process. First, it directly reminds us that making laws and policy is a hard, sometimes unseemly business, that may be unpalatable to observe but which has many admirable and deeply practical objectives; after all, every society needs metaphorical sausages—good policy and good law. But the story also serves, at a meta-level, as a cautionary tale that all of the things we think we know to be true aren't necessarily so; and this is especially true in the realm of cyberspace.

---

* Principal, Red Branch Consulting PLLC; Carnegie Fellow in National Security Journalism, Medill School of Journalism, Northwestern University (2011); Professorial Lecturer in Law, George Washington University. The author served as Deputy Assistant Secretary for Policy in the Department of Homeland Security from 2005-09. Portions of this article will appear in the forthcoming book *Cyberwarfare: How Conflicts in Cyberspace are Challenging American and Changing the World* (Santa Barbara: Praeger, 2012). I am indebted to the participants at the Ohio State University symposium "Cybersecurity: Shared Risks, Shared Responsibilities" and particularly to Jeffrey Hunker and Peter Shane for their thoughtful comments on an earlier version of this paper.

[1] Fred R. Shapiro, "Quote … Misquote," *The New York Times*, July 21, 2008, http://www.nytimes.com/2008/07/21/magazine/27wwwl-guestsafire-t.html.

Put another way, there are two different types of things that can go wrong when Washington policy makers make cyber policy. One class of mistake is analytically uninteresting (at least in the context of this symposium)—they are the types of errors that are common to all sorts of policy making in Washington today. There is a robust, detailed academic literature on these types of problems: the difficulties of rent-seeking in a regulated environment; the prevalence of information asymmetries amongst actors; parochialism in decision-makers; and the like. These are problems that are familiar to all our policymakers and there is nothing unique about the cyber domain that exempts it from these challenges. To put it prosaically and to cite but one example of many, major telecommunications providers are neither more nor less likely to lobby to protect their own financial interests when the subject is cybersecurity than they are to seek favorable decisions in the areas of telephony or cable access. And, precisely because these challenges are no different for cyber policy than in any other field they aren't terribly interesting in the context of a symposium on cybersecurity policy. Other than noting them in passing here, and without in any way minimizing the difficulties that this sort of behavior poses for making good policy, I don't propose to discuss them further.

Instead, this brief essay will focus on two more interesting questions: First, whether or not there is a class of issues and challenges in policy making that is unique to the cyber domain; and second, whether there are issues that, if not unique, are more predominant or readily apparent in the context of cyber policy making than in other areas of governmental endeavor.

I submit that the answer to the question is "yes" on both accounts. There are unique challenges that arise from the nature of the cyber domain and from the failure of policy makers to adequately understand and adapt to that nature. Two aspects of that nature in particular have yet to be comprehended: the cyber domain's ubiquity and rapidity; and its asymmetric empowerment.

Relatedly, there is a class of challenges that, though not unique to the cyber domain are significantly exacerbated in that domain. These are the types of challenges that are predominant in most public policy making involving developing science and technology. They involve the rapidity of change, policy makers' lack of familiarity with the technology under development, and the unpredictability of future developments.[2] Our policy makers have yet to come to grips with the

[2] In 2010, the author attended a senior level military cyber exercise at the Army War College. The challenge of dealing with new technology that leaders did not understand was

transformative scope of the technology and thus they have yet to modify the policymaking apparatus to the reality of cyber systems.

II. UNIQUE ASPECTS OF CYBERSPACE -- UBIQUITY AND RAPIDITY

"The internet destroys both time and space."[3] It is both global in scope and near-instantaneous in operation. Until policy makers understand and adapt to this unique environment they cannot readily respond to it.

A. UBIQUITY

Cyberspace is everywhere. It pervades our economy and our critical infrastructure. For example, the Department of Homeland Security has identified eighteen sectors of the economy as the nation's critical infrastructure and key resources.[4] This comprehensive list covers everything from transportation to the defense industrial base. It includes energy, financial systems, water, agriculture, and telecommunications**.** Remarkably, virtually all of the sectors now substantially depend on cyber systems. Even those activities most solidly grounded in the physical world—such as manufacturing or food production—have become reliant on computer controls and access to the World Wide Web of information. Manufacturing systems are controlled by computer systems operated at a distance through virtual connections; farmers use global positioning system tracking, satellite data, and just-in-time ordering to maintain their operations. The list goes on.

At the same time, cyber systems have come to underpin many of our social interactions. The cyber domain enables Facebook as a social network and Twitter as an information source. Blogging and internet video viewing are growing at an exponential pace and may soon exceed television viewing and newspaper reading. Indeed, today,

---

well-encapsulated in the advice that was given to the attending senior officers: "If your cyber-advisor is older than 35, you need a new advisor."

[3] Remarks of Kim Taipale, Duke University Center on Law, Ethics and National Security (April 2010), http://www.law.duke.edu/lens/conferences/2010/program.

[4] For a complete list, see Department of Homeland Security, "Critical Infrastructure and Key Resources Sectors,"
http://training.fema.gov/EMIWeb/IS/IS860a/CIKR/sectorMenu.htm.

according to Internet World Stats, the number of Internet users exceeds two billion, more than 30% of the world's population.[5]

In short, one fundamental characteristic of the Internet that makes it truly different from the physical world is that it lacks any boundaries. This creates a profound challenge for American policy makers because their background is almost wholly derived from a state-based system of sovereignty that is bounded in geographic space. By contrast the reality is that cybersecurity is boundless and, thus, inevitably, an issue of global concern.

In short, you can't be an American isolationist and make good cyber policy. Significant instances of espionage have originated overseas.[6] Some countries, such as Russia and Ukraine, have become known as safe havens for cyber criminals.[7] It can be anticipated that if there ever is a cyber war, America's enemies will launch their attacks from overseas sites that, initially, are beyond U.S. control.

Some countries have responded to this reality by attempting to cut themselves off from the Internet or censor traffic arriving at their cyber borders. The most notorious example is China's attempt to construct a "Great Firewall" to keep Internet traffic out of the country.[8] China conducts an active effort to suppress adverse news on the Internet, with more than three hundred thousand Internet monitors engaged in the process.[9] As a result the recent unrest in the Middle East seems to be unable to find traction in China. The instinct to regulate is not, however, limited to authoritarian régimes—even

---

[5] Statistics regarding worldwide Internet usage are compiled by Internet World Stats, http://www.internetworldstats.com/stats.htm. This is an increase from just sixteen million in 1995.

[6] Public reports of the contents of cables released by Wikileaks suggested Chinese complicity in several extensive cyber exploits. James Glanz and John Markoff, "Vast Hacking by a China Fearful of the Web," *New York Times*, December 4, 2010, http://www.nytimes.com/2010/12/05/world/asia/05wikileaks-china.html. The underlying cables remain classified and the government has directed those people (including this author), who have an active security clearances, to refrain from reviewing the substance of the cables.

[7]John Barnham, "Russia's Cybercrime Haven," *Security Management*, November 2008, http://www.securitymanagement.com/article/russias-cybercrime-haven-004818.

[8] To "test any website and see real-time if it's censored in China," see Great Fire Wall of China, http://www.greatfirewallofchina.org.

[9] L. Gordon Crovitz, "Opinion: Dictators and Internet Double Standards," *Wall Street* Journal, March 7, 2011, http://online.wsj.com/article/ SB10001424052748703580004576180662638333004.html.

liberal Western countries like Australia have proposed restrictions on Internet traffic, albeit for facially more legitimate reasons, such as limiting the spread of child pornography.[10]

But such strategies are, in the end, bootless. In the long run, they will prove ineffective, and to the extent they are effective, they cut countries off from the benefits of the Internet. The salient feature of the cyber domain is precisely its ability to accumulate and integrate large bodies of information over long distances in an instant. Any country that erects effective cyber borders is systematically agreeing to forgo those benefits, to its own detriment. While that might be feasible for a totalitarian state, it will never work for America. And so, inevitably, we are likely to remain deeply entwined in the global network of cyberspace.

The problem, however, is that our policy structures and concepts are not well suited to this reality. American tradition, going back literally to our founding era, is about avoiding foreign entanglements.[11] We have, justifiably, a skeptical view of international organizations and solutions.

Yet, because the cyber problem is a global one, America's strategy must be to engage internationally, both cooperatively with friends and allies, and punitively with those who refuse to prevent crime and espionage at locations within their effective control. This will require a greater willingness to share information and cooperate with appropriate allies (such as the U.K.). America's primary focus should be on working cooperatively thorough existing bilateral partnerships and engaging effective international organizations (like NATO).[12] In addition, the United States may need to take the lead in the development of international norms and rules that presumptively

---

[10] Associated Press, "Australia Says Web Blacklist Combats Child Porn," *Physorg.com*, March 27, 2009, http://www.physorg.com/news157371619.html.

[11] The most famous instance of this tradition, of course, is George Washington's Farewell Address in 1796. "George Washington's Farewell Address in 1796," The Avalon Project—Lillian Goldman Law Library, http://avalon.law.yale.edu/18th_century/washing.asp. In his farewell address, Washington warned his fellow citizens to "steer clear of permanent alliances" and counseled that the "great rule of conduct for us in regard to foreign nations is in extending our commercial relations, to have with them as little political connection as possible. … [I]t must be unwise in us to implicate ourselves by artificial ties in the ordinary vicissitudes of her politics, or the ordinary combinations and collisions of her friendships or enmities."

[12] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October 2010, 97, http://www.cfr.org/publication/22849/defending_a_new_domain.

assign liability to countries that harbor hackers (like Russia and China). The policy mind-set we have today isn't quite ready for that sort of engagement.

B. RAPIDITY

Cyber world is also a world of rapidity. The speed at which events can happen in the cyber domain makes real world events seem lugubrious; not only does the cyber domain span the globe, but it does so in a near instantaneous fashion. There is no kinetic analog for this phenomenon—even the most global-spanning weapons, like missiles, take thirty-three minutes to reach their distant targets.

The concept of rapidity causes two distinct problems for policy makers. Both are directly tied to the pace of action in cyberspace but, confusingly, they point in opposite directions. On one hand, the pace of action in cyberspace may seduce policy makers into believing that a near-instantaneous response is necessary when, in fact, a more measured response would be preferred. On the other hand, the speed of events may leave decision makers far behind as their processes for policy making are too slow to allow a timely response—a problem that is not unique to cyberspace but it is exacerbated by its effects. The difficulty in distinguishing the two circumstances is a confounding factor that measurably complicates the challenge of dealing with cyber rapidity.

C. THE NANO-SECOND POLICY

The rapidity of action in cyberspace teaches some policy makers a lesson about the need to discard policy-making hierarchy. Reasoning that human decisionmaking is too slow for cyberspace, they conclude that rapidity of response will be the hallmark of cyber policy. This is particularly true in the context of cyber warfare: When a cyber domain attack or intrusion is perceived to occur at the pace of milliseconds, some theorists argue that a response will need to occur with equal rapidity.

As then-Lieutenant General Keith Alexander, the first Commander of U.S. Cyber Command, told the Senate during his confirmation hearings, "[A] commander's right to general self-defense is clearly established in both U.S. and international law. Although this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with the law of war principles (e.g.

proportionality), would be lawful."[13] And what this means is that some of the most influential leaders in the development of cyberspace policy think that the need to respond immediately will necessarily drive decision making down to lower levels in the chain of command.

Indeed, if you think that instantaneous self-defense is a necessity this leads to the development of policy making requirements that will inevitably result in important decisions being taken by subordinate officials. To put it in a simplistic fashion, under this policy construct the decision to go to cyber war with China may be made, not by the President, but by a senior General who thinks that his command and control system is under attack and elects to fire back.

There is good reason, however, to question whether the assumptions of rapidity that lie behind the policy structure for responding to attacks or intrusions are correct. As Martin Libicki pointed out in a recent RAND study, a cyber response is unlikely to be able to disable a cyber attacker completely. As a consequence, for policy, "[m]ore important than [the] speed [of the response] is the ability to convince the attacker not to try again. Ironically, for a medium that supposedly conducts its business at warp speed, *the urgency of retaliation is governed by the capacity of the human mind to be convinced, not the need to disable the attacking computer before it strikes again.*"[14]

In some ways, this problem for the development of policies in the cyber domain is akin to analogous challenge faced in other domains. The issue is "how to sustain human control [that is, maintain a] man-in-the-loop. . . . For example, control structures can have human control to unlock weapons systems, or automatic system unlock with human intervention required to override. An example of the former is the control of nuclear weapons and of the later, the control of a nuclear power reactor. This may be high tech, but the big questions are political and organizational."[15] Indeed, the problems associated with internet rapidity and with the lack of human control structures or

---

[13] "Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander," United States Cyber Command in Hearings Before the United States Senate Armed Services Committee, 24 (April 13, 2010), http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf; Lynn, "Defending a New Domain," 103 (The U.S. military must "respond to attacks as they happen or even before they arrive.").

[14] See Martin Libicki, "Cyberdeterrence and Cyberwar," 62, RAND (2009), http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf (emphasis supplied).

[15] Tom Blau, "War and Technology in the Age of the Electron," *Defense Security Review* 94 (1993): 100.

policy were demonstrated, in a painful fashion, recently when automated trading rules caused a "flash crash"—a thousand point decline in the Dow Jones Industrial Average in less than ten minutes of trading on the New York Stock Exchange.[16] If we are going to avoid similar, more harmful failures (one can, for example, imagine a "flash war"), policy makers will need to come to grips with and learn to defuse the incessant rapidity of cyberspace.

D. THE POLICY "FORD SEDAN"

By far the more common phenomenon (at least in my own limited experience) arises when the pace of events in cyberspace moves so quickly that policy cannot keep up.[17] The problem, here, is a structural one, rather than a systematic substantive challenge and is more common whenever technological change needs to be accounted for. Put simply, policy is made through policymaking institutions and our institutions are bounded by existing processes and inherent limitations. In a world in which notice and comment rulemaking[18] takes eighteen to twenty-four months[19] to complete —during which

---

[16] Nelson Schwartz and Louise Story, "Surge of Computer Selling After Apparent Glitch Sends Stocks Plunging," *New York Times*, May 7, 2010, http://www.nytimes.com/2010/05/07/business/economy/07trade.html?sq=machines%20take%20control%20may%207%202010&st=cse&adxnnl=1&scp=1&adxnnlx=1311103991-oZnL8wRwWUXpqTGUEXyisQ.

[17] As I've said, this problem is common to many science and technology questions. It may also, amusingly, arise in connection with more prosaic social phenomenon: "Fitness fads change too quickly for anyone to keep up with all of them." NU FitRec at 2 (Spring-Summer 2011) (on file with author).

[18] The Administrative Procedures Act requires new rules and regulations to be subject to notice to the public and comment thereon. 5 U.S.C. § 551 *et. seq*.

[19] This is, of course, just an estimate. One study, Stuart Shapiro,, "Explaining Ossification: An Examination of the Time to Finish Rulemakings" (working paper, Social Science Research Network, August 11, 2009), http://ssrn.com/abstract=1447337, estimated that the median time for completion of a rule, from its first appearance in the Unified Agenda to promulgation was 618 days, while the mean was 831 (or 27+ months). If one counts from the date the rule is first formally proposed the mean is only 324 days, but my own experience is that significant rules require substantial pre-proposal consideration and consultation. For complex rules that will engender significant comment (as we can anticipate will be the case with cyber rules) my assumption is that longer periods of consideration will be necessary more frequently than shorter periods.

time the average processing speed of computer chips will have doubled—our system for making policy is ill-suited to the task.[20]

Any number of examples of this phenomenon could readily be cited, but the recent revolutionary movements in the Middle East are a particularly good example of the accelerating pace of events enabled by cyberspace. The Internet gives non-state actors the ability to communicate rapidly and organize (to, in effect, have an organic command and control system) that begins to rival that of sovereigns.

Consider: On January 25, the people of Egypt took to the streets in a "day of rage," protesting the rampant poverty, unemployment, and government corruption seen throughout the country. The young rebels in the crowds used social media to mobilize the people. One Facebook page dedicated to a protest, for instance, had over eighty thousand followers.[21] Through exchanges with Tunisian protesters, they learned how to reduce the effects of tear gas on their eyes by putting "vinegar or onion under your scarf."[22] And the origins of the resistance lay even more deeply in social coordination—bloggers in Egypt tried to organize local strikes against the government and they, in turn, energized youthful bloggers in Tunis.

The governments in the Middle East were slow to respond and did so with little subtlety. One day after the revolt in Egypt started Facebook, Twitter, Gmail, and YouTube were shut down, and the cell phone company Vodaphone suspended service. The day after that Egypt's five main Internet service providers cut off international access to their customers.[23] While the government claimed it was not

---

[20] Though the rapidity of action in cyberspace greatly exacerbates the problems of hierarchy in our policy-making process, those problems are not limited to cyber issues. As the Project for National Security Reform put it in a recent report: "The legacy structures and processes of a national security system that is now more than 60 years old no longer help American leaders to formulate coherent national strategy. … As presently constituted, too, these structures and processes lack means to detect and remedy their own deficiencies." Project for National Security Reform, *Forging a New Shield*, November 2008, http://pnsr.org/data/files/pnsr_forging_a_new_shield_report.pdf, i.

[21] Maggie Michael, "Egyptians Plan First Tunisian-Inspired Protests, Draw 80,000 Supporters on Facebook," *StarTribune*, January 24, 2011, http://www.startribune.com/world/114479579.html.

[22] David D. Kirkpatrick and David E. Sanger, "A Tunisian-Egyptian Link that Shook Arab History," *New York Times*, February 13, 2011, http://www.nytimes.com/2011/02/14/world/middleeast/14egypt-tunisia-protests.html?_r=1&ref=todayspaper.

[23] Christopher Rhodes and Geoffrey A. Fowler, "Egypt Shuts Down Internet, Cell Phone Service," *Wall Street Journal*, January 29, 2011, http://online.wsj.com/article/SB10001424052748703956604576110453371369740.html.

responsible for killing the Internet, efforts seemed targeted specifically to quell the uprising. A few days later, the government apparently gave up, restoring service.[24]

Within a few short weeks, Mubarak had been ousted from his Presidency and Egypt began a transition to some new form of government, though the final resolution of the Egyptian crisis has yet to be determined. Social media services have come back on line, and appear to be a continuing part of the effort to transform the country. And Egypt may only be the start of a larger phenomenon. As one leader in Egypt, Walid Rachid, said: "Tunis is the force that pushed Egypt, but what Egypt did will be the force that will push the world." He, and others in his movement, dream of sharing their experiences with similar youth movements in Libya, Algeria, Morocco and Iran.[25] These unfolding events are a vivid example of how the cyber domain creates social change at a dizzying pace—in this case, to quite literally challenge a sovereign government backed by law enforcement and military power. Not only were the Middle Eastern nations unable to adapt, but one has a clear sense that our own policy-making in the United States was left behind the curve of events. For weeks, as the democracy movement grew, America was slow to respond, leaving many to wonder if our diplomacy was "too little, too late."[26] To be sure, the shock of change in the Middle East might have overwhelmed our decision making even at a slower pace; but there can be little doubt that the cyber-infused rapidity of events made the job significantly more challenging.

* * * * *

A number of other cyber examples of this phenomenon can be readily identified. Here are a few as follows: Product life cycles in the cyber domain are notoriously short. New chips, new processors, and

---

[24] Shereen El Gazzar, "Government Restores Internet Service After a Weeklong Shutdown," *Wall Street Journal*, February 2, 2011, http://online.wsj.com/article/SB10001424052748703960804576119690514692446.html.

[25] Kirkpatrick and Sanger, "Egyptians and Tunisians Collaborated to Shake Arab History" (see n. 22).

[26] Literally dozens of articles could be cited for the proposition. For a relatively non-tendentious example see Rachel Newcomb, "Why Obama's Position on Egypt's Mubarak Was Too Little, Too Late," *Christian Science Monitor*, February 2, 2011, http://www.csmonitor.com/Commentary/Opinion/2011/0202/Why-Obama-s-position-on-Egypt-s-Mubarak-was-too-little-too-late.

new software are released on a seeming continuous basis. One good example of our inability to deal with the rapidity of events in cyberspace is our systematic failure to develop a procurement system that allows the purchase of cutting edge information technology for our military.[27] Despite years of effort to streamline the process, we still face the "fundamental problem … that the deliberate process through which weapon systems and information technology are acquired does not match the speed at which new IT capabilities are being introduced into today's new information age."[28]

Similarly, our response to cyber crime has been mired in traditional modes of international cooperation. The Council of Europe Convention on Cybercrime[29] creates two distinct yet interrelated obligations on its signatories. First, every nation signing the Convention is obligated to adopt criminal law provisions that substantively punish those who illegally access or use computers. Second, each nation is also obliged to adopt procedures for sharing information about criminal activity, preserving evidence and extraditing identified offenders. As with most such conventions, the precise contours of these substantive and procedural laws are left to the discretion of each signatory.

But the Convention's provisions and procedures are widely regarded as unpopular, ineffective, slow, and cumbersome. It took years to negotiate the Treaty and today, eight years after its adoption, only 27 countries have ratified it (while several whose cooperation is necessary in any global regime—most notably China and Russia—have refused to accede to the Treaty). The convergence of criminal law has been a slow process. Significant cultural and legal hurdles (e.g. differing American and European approaches to "hate" speech) have further delayed the effort.

More importantly, the Treaty relies on outmoded means of information exchange, including a process of Mutual Legal Assistance Treaties (MLATs) and "letters rogatory" that dates back to the 18th century. As three senior PayPal executives recently explained: "In all of the cases where we have worked with multi country investigations, we have *never* seen a case in which the data has been returned to the

---

[27] See Defense Science Board, *Department of Defense Policies and Procedures for the Acquisition of Information Technology*, March 2009, http://www.acq.osd.mil/dsb/reports/ADA498375.pdf.

[28] *Ibid*.,3 (Memorandum from William Schneider, Jr., DSB Chairman).

[29] The treaty was first adopted in 2001. Its text is available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

requesting law enforcement agency in under three months. Six months is more common, and we have heard of cases where the data has been returned more than two years after it was originally requested."[30] If ever there wasa perfect example of how policy and law have not kept up with the pace of cyber reality, this would be it. The Treaty would be far more effective had it adopted more rapid response mechanisms that work in real-time. The technology for such an effort is readily available in the current interconnected environment.

Finally, consider the Administration's recent cybersecurity legislative proposal.[31] This proposal was, itself, the product of many years work, dating back to the Bush Administration. Within the current Administration it was more than two years in the crafting—something to be expected given the complexity of the topic and the significant equities at issue.

But the very slowness of that process will, quite possibly, be the downfall of the proposal. Some of it was outdated even before it was proposed. For example, the Administration draft relies heavily on authorization for the deployment of an intrusion detection and prevention system.[32] But cyber experts are generally of the view that intrusion systems are becoming out of date. As one expert, put it: "The attackers are two years ahead of the defenders, security vendors, who are two years ahead of market, which is two years ahead of compliance, and legislation is five years behind that....These practices may be even more stale once enacted. It's unlikely the law could ever keep pace, given the glacial pace of legislation."[33]

In short, our hierarchical decision-making structures remain dominant and operate far too slowly to catch up with the pace of cyber activity. Our policymaking apparatus can't turn inside the cyberspace innovation radius. Or, as one of my colleagues has put it, the

---

[30]Barrett, Steingruebel, and Smith, *Combating Cybercrime: Policies, Principles and Programs*,, April 2011, ,https://www.paypal-media.com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4.pdf, 16-17 (emphasis in original).

[31] The text of this draft proposal, transmitted to Congress in May 2011, is available at http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf.

[32] *Ibid*., 24.

[33] "White House Cybersecurity Plan Feared Inadequate By Experts, Could Violate Privacy," E-commercealert.com, May 17, 2011,, http://www.e-commercealert.com/article1067.shtml (quoting Josh Corman, Research Director, 451 Group).

government is using a "Ford sedan" policymaking system to manage the cyberspace "Porsche" system.[34]

* * * * *

In the end, then, the issue of rapidity seems to look in two directions at the same time. On one hand, we need structures in place that slow down our responses in time of crisis and allow the time for mature consideration lest we overreact to a situation in haste. On the other hand, as is often the case when technological change is at hand, some of our long-term policy making structures are so slow-moving that we risk being left behind, caught up in a mode of thought (built when sovereign states acted in a kinetic world) that no longer reflects the dominant reality of our new systems.

III. ASYMMETRIC EMPOWERMENT

The other piece of the puzzle lies in the unique capacity of cyberspace to allow and enable individuals (or groups of individuals) to compete with more established social institutions. We see this happening around the world with increasing frequency, and governmental institutions have only begun to realize what a challenge is posed to their monopolies on information and power by the growth of the Internet. A rough taxonomy of the issue would identify at least three distinct ways in which this sort of asymmetric empowerment can be effectuated: through better coordination (as seen in the Middle East example just noted); through greater access to information; and through the enablement of non-state actors to compete directly with sovereigns.

One vivid example (and one that may portend significant challenges to the hegemony of the current social order) lies in the two-stage challenge to social authority arising from the events surrounding WikiLeaks and its founder, Julian Assange. Their story is one of both enhanced information transparency and, in the end, the ability to wage combat in cyberspace.

---

[34] I am indebted to Professor Harvey Rishikof, Chair of the American Bar Association Standing Committee on Law and National Security, for this wonderful image. Quoting him also illustrates the proposition in a self-referential way. Like many in Washington, Professor Rishikof also has a government affiliation. If I had wanted to identify him by that affiliation, he would have required a week or more to get the requisite clearances from other officials. As a private sector actor, he authorized reliance on his imagery immediately.

A. "NO MORE SECRETS"

The transparency aspect of the story is well known and widely remarked on. Using a series of servers and an anonymization protocol WikiLeaks accepts and publishes documents provided to it by sources within governments.[35] Though the site has published documents with provenance as wide ranging as Zambia and Abu Dhabi, its most notable (or perhaps notorious) publications have involved a number of American documents, including the video of a war-time friendly fire incident, raw tactical intelligence from the battlefields of Iraq and Afghanistan, and a trove of classified State Department cables.[36]

Opinions vary as to the efficacy of WikiLeaks transparency efforts. To be sure some of the most apocalyptic predictions (that nobody would talk to American diplomats ever again) have proven over blown. On the other hand, reliable reports suggest that the WikiLeaks disclosures have had significant public repercussions, ranging from increased tensions in US-Mexican relations,[37] to threats to the leader of the Zimbabwean opposition leader,[38] to reports that the Taliban have collated a list of people who helped the United States and have targeted them for killing.[39] Indeed, some analysts have even said that the public disclosure of America's opinion of the Tunisian leader played a role in catalyzing the Tunisian rebellion that sparked the current surge in Middle East unrest.[40] It would be easy to overstate

---

[35] A more detailed description of how WikiLeaks achieves technical anonymity can be found at WikiLeaks, "About WikiLeaks," http://www.wikileaks.ch/About.html. WikiLeaks asserts that it does not solicit disclosures and declines to disclose details of its submission process in order to avoid "compromise" of the organization.

[36] For an account of Wikileaks association with the *New York Times*, see Bill Keller, "Dealing With Assange and the WikiLeaks Secrets," *New York Times*, January 30, 2011, http://www.nytimes.com/2011/01/30/magazine/30Wikileaks-t.html?ref=todayspaper.

[37] Mary Beth Sheridan, "Calderon: WikiLeaks Caused Severe Damage to U.S.-Mexico Relations," *Washington Post*, March 3, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/03/03/AR2011030302853.html?wpisrc=nl_buzz.

[38] David Smith, "Morgan Tsvangirai Faces Possible Zimbabwe Treason Charge," *The Guardian*, December 27, 2010, http://www.guardian.co.uk/world/2010/dec/27/wikileaks-morgan-tsvangirai-zimbabwe-sanctions?CMP=twt_gu.

[39] Keller, "The *Times*' Dealings With Julian Assange," 9.

[40] Maha Azzam, "Opinion: How WikiLeaks Helped Fuel Tunisian Revolution," CNN.com, January 18, 2011, http://articles.cnn.com/2011-01-18/opinion/tunisia.wikileaks_1_tunisians-wikileaks-regime?_s=PM:OPINION.

the case, but it seems clear that we increasingly live in a world where secrecy is losing ground to transparency, with significant effects.[41]

To be sure, this problem is not unique to cyberspace. But the availability of transparency enhancing technology in the cyber domain will increase the frequency and salience of transparency in our public discourse. Put simply, there is a significant difference in degree between the leak of the *Pentagon Papers*[42] to the New York Times and the massive data-dumps practiced by WikiLeaks. This difference in degree borders on a difference in kind and it will require a sea-change in how our national security system operates—one for which it is not well-prepared.

As a recent American Bar Association report put it: "The national security community traditionally relies upon information monopoly providing it with strategic advantage. This assumes that that the government has information that its competitors or adversaries do not. Given the ubiquity of information in open sources, the irresistible benefits that come from networking information, and the vulnerability of cyberspace, this assumption should be seriously challenged inside and outside of government. It is increasingly likely that others will have the same information, either because they have stolen it from you or because they have been able to develop it independently."[43] Policy makers (especially in the national security domain) have long been accustomed to making policy behind closed doors and our structures for policy making presume that capacity. Though, to be sure, we have long had to accommodate the process to occasional leaks of information (some of great significance) the transparency of cyberspace reflects a quantum change in those expectations for which our policymaking institutions are not ready.

B. NO MORE SOVEREIGNS?

---

[41] Scott Shane, "Keeping Secrets WikiSafe," *New York Times*, December 11, 2010, http://www.nytimes.com/2010/12/12/weekinreview/12shane.html?_r=1&scp=5&sq=wikileaks&st=cse.

[42] National Archives, *Report of the Office of the Secretary of Defense Vietnam Task Force*, 1967,, http://www.archives.gov/research/pentagon-papers.

[43] American Bar Association Standing Committee on Law and National Security, *No More Secrets: National Security Strategies for a Transparent World*, March 2011, http://www.americanbar.org/content/dam/aba/administrative/law_national_security/no_more_secrets2.authcheckdam.pdf, 4.

The second part of the story, and perhaps the more interesting part, revolved around the reaction to Mr. Assange's arrest in Great Britain and the decision of many companies to sever financial relationships with Wikileaks. What happened next was novel. As Professor Clay Shirky has put it: "The competitive landscape [got] altered because the Internet allow[ed] insurgents to play by different rules than incumbents."[44]

Confronted with WikiLeak's anti-sovereign slant, the institutions of the traditional status quo soon responded. Of course, none of the governments ordered any actions (or, more accurately, none is known to have), but the combination of governmental displeasure and public relations disdain soon led a number of major Western corporations (MasterCard, PayPal, and Amazon, to name three) to withhold services from WikiLeaks. Amazon reclaimed rented server space that WikiLeaks had used and the two financial institutions stopped processing donations made to WikiLeaks.[45]

What soon followed might well be described as the first cyber battle between non-state actors. Supporters of WikiLeaks, loosely organized in a group under the name "Anonymous" (naturally) began a series of distributed denial-of-service (DDoS) attacks on the web-sites of the major corporations that they thought had taken an anti-WikiLeaks stand.[46] The web site of the Swedish prosecuting authority (who is seeking Mr. Assange's extradition to Sweden to face criminal charges) was also hacked. Some of the coordination for the DDoS attacks was done through other social media, such as Facebook or Twitter.[47] Meanwhile, other supporters created hundreds of mirror

---

[44] Clay Shirky, "From Innovation to Revolution," *Foreign Affairs*, March 2011, http://www.foreignaffairs.com/articles/67325/malcolm-gladwell-and-clay-shirky/from-innovation-to-revolution?cid=emc-mar11promoa-content-030811.

[45] Ashlee Vance, "WikiLeaks Struggles to Stay Online After Cyberattacks," *New York Times*, December 3, 2010, http://www.nytimes.com/2010/12/04/world/europe/04domain.html?_r=1&ref=world.

[46] John F. Burns and Ravi Somaiya, "Hackers Attack Those Seen As WikiLeaks Enemies," *New York Times*, December 8, 2010, http://www.nytimes.com/2010/12/09/world/09wiki.html?ref=todayspaper; Joby Warrick and Rob Pegoraro, "WikiLeaks Avoids Shutdown as Supporters Worldwide Go On the Offensive," *Washington Post*, December 8, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/08/AR2010120804038.html?hpid=moreheadlines.

[47] Ashlee Vance and Miguel Helft, "Hackers Give Web Companies a Test of Free Speech," *New York Times*, December 8, 2010, http://www.nytimes.com/2010/12/09/technology/09net.html?_r=1&hp.

sites, replicating WikiLeaks content, so that it couldn't be effectively shut down.[48] The hackers even adopted a military-style nomenclature, dubbing their efforts "Operation Payback."

And the other side fought back. The major sites used sophisticated cybersecurity methodology to oppose the Anonymous attacks. Most attacks were relatively unsuccessful—the announced attack on Amazon, for example, was abandoned shortly after it began because the assault was ineffective. Perhaps even more tellingly, someone (no group has, to my knowledge, publicly claimed credit) began an offensive cyber operation against Anonymous itself. The group which ran its operations through a website, AnonOps.net, was subject to DDoS counterattacks that took it offline for a number of hours.[49] In short, a conflict readily recognizable as a battle between competing forces took place in cyberspace waged, exclusively between non-state actors.[50]

The failure of Anonymous to effectively target corporate web sites and its relative vulnerability to counter-attack are, I think, only temporary circumstances. They (and their opponents) will learn from this battle and approach the next one with a greater degree of skill and a better perspective on how to achieve their ends. Indeed, since the initial PayPal attacks, a low-grade conflict has continued—the CIA website has been attacked by LulzSec (another hacktivist group)[51] and Anonymous hacked the government contractor, Booz Allen Hamilton

---

[48] Ravi Somaiya, "Hundreds of WikiLeaks Mirror Sites Appear," *New York Times*, December 6, 2010., http://www.nytimes.com/2010/12/06/world/europe/06wiki.html?_r=1&ref=world.

[49] Christopher Walker, "A Brief History of Operation Payback," Salon.com, December 9, 2010, http://www.salon.com/news/feature/2010/12/09/0.

[50] The sovereign states were not, of course, mere bystanders. Dutch police, for example, arrested one suspected member of Anonymous. Tim Hwang, "WikiLeaks and the Internet's Long War," *Washington Post*, December 12, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/12/10/AR2010121002604.html?hpid=opinionsbox1. The Spanish recently arrested three more, charged with the Sony Play Station hack. David Jolly and Raphael Minder, "Spain Detains 3 in PlayStation Cyberattacks," *New York Times*, June 10, 2011, http://www.nytimes.com/2011/06/11/technology/11hack.html?_r=2. And, nobody can be certain that the counter-attacks on AnonOps.net were not state-authorized or state-initiated.

[51] Mathew J. Schwartz, "LulzSec Claims Credit for CIA Site Takedown," Informationweek.com, June 16, 2011, http://www.informationweek.com/news/security/cybercrime/230800019.

stealing 90,000 email addresses and passwords.[52] In return, governments have moved against the groups, recently arresting 16 members of Anonymous and charged them with crimes in connection with the original PayPal attack.[53]

Anonymous has made quite clear that it intends to continue to prosecute the cyberwar against, among others, the United States. "It's a guerrilla cyberwar—that's what I call it," according to Barrett Brown, 29, a self-described senior strategist and "propagandist" for Anonymous.[54] "It's sort of an unconventional asymmetrical act of warfare that we're involved in, and we didn't necessarily start it. I mean, this fire has been burning." Or, consider, the manifesto posted by Anonymous, declaring cyberspace independence from world governments: "I declare the global social space we are building together to be naturally independent of the tyrannies and injustices you seek to impose on us. You have no moral right to rule us nor do you possess any real methods of enforcement we have true reason to fear."[55] In advancing this agenda, the members of Anonymous look very much like the anarchists who led movements in the late 19th and early 20th centuries—albeit anarchists with a vastly greater network and far more ability to advance their nihilistic agenda through individual action.[56]

This is a novel challenge to the traditional model of conflict between state actors. The problem of dealing with non-state actors

---

[52] Nancy Gohring, "Anonymous Hacks Booz Allen, Posts 90K Email Addresses and Passwords," ComputerWorld.com, July 11, 2011, http://www.computerworld.com/s/article/9218328/Anonymous_hacks_Booz_Allen_posts_90K_military_email_addresses_and_passwords.

[53] Jana Winter, "16 Suspected 'Anonymous' Hackers Arrested in Nationwide Sweep, Foxnews.com, July 19, 2011, http://www.foxnews.com/scitech/2011/07/19/exclusive-fbi-search-warrants-nationwide-hunt-anonymous.

[54] Michael Isikoff, "Hacker Group Vows 'Cyberwar' on U.S. Government, Business," msnbc.com, March 8, 2011, http://www.msnbc.msn.com/id/41972190/ns/technology_and_science-security.

[55] The manifesto was posted as a YouTube video: "Anonymous to the Governments of the World," YouTube.com, April 25, 2010, http://www.youtube.com/watch?v=gbqC8BnvVHQ.

[56] See Abe Greenwald, "The Return of Anarchism," *Commentary*, March 2011, 32.. One possible additional point of comparison is that the 19th century anarchists were well known for their internal disputes. Much the same may happen to Anonymous, as recent reports of internal divisions suggests. "Trouble in Paradise for Hacker Group Anonymous?," ITAC Blog, March 23, 2011, http://itacidentityblog.com/trouble-in-paradise-for-hacker-group-anonymous.

like Anonymous resembles, in structure, the problem of dealing with a non-state insurgency on the ground in Iraq or Afghanistan. But, there are significant differences between the two domains. In the "kinetic" world, the goal of an insurgency is often the overthrow of an existing government. As the U.S. Army's Counterinsurgency Field Manual puts it: "Joint doctrine defines an *insurgency* as an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict. An insurgency is an organized, protracted politico–military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control."[57] In other words, the kinetic insurgency is grounded in the traditional conception of sovereignty.

The cyber-insurgency is not. Anonymous-like insurgents seem to have a different aim—"independence" from government. That independence is premised on weakening political authority over the cyber domain. Given the difference in goals, our policy makers will need to learn to deal with a different reality. Operationally, the cyber-insurgency challenges pose many of the same problems as do kinetic insurgencies—how to isolate fringe actors from the general populace and deny them support and refuge and, most of all, the freedom to attack at the time and place of their choosing. But strategically, the differences will be significant.

The hegemony of nation-states has been the foundation for international relations since the Peace of Westphalia.[58] The natural first reaction of those nation-states will be an effort to reassert their sovereignty over the internet.[59] But their success in those efforts is radically contingent, and it may be that the better policy is to adapt rather than to resist the changes wrought by the asymmetry of cyberspace. Here, as with the ubiquity problem, our decision makers are bound up in a conception of the world that isn't readily susceptible to change and may constrain our ability to make good policy.

---

[57] Department of the Army, "Counterinsurgency," FM 3-24, December 2006, 1-2, http://www.fas.org/irp/doddir/army/fm3-24.pdf.

[58] The Treaty of Westphalia, signed in 1648, ended the 30-Years War. It is often considered the international agreement that recognized the sovereignty of nation states. The text of the treaty is available at http://avalon.law.yale.edu/17th_century/westphal.asp.

[59] Chris C. Demchak and Peter Dombrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 32 (Spring 2011), http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf.

IV. CONCLUSION

If the question about cyberspace is: "What is our policy making apparatus most likely to misunderstand or get wrong?" the answer, I fear, is quite a lot. Not because policy makers in Washington are ill-meaning, or venal, or even unintelligent. But rather, I fear, because they are confronting a new reality to which they have yet to adapt. The sausage making process of policy development inside sovereign governments is slow and encrusted with hierarchical restrictions. It lacks the pace and capacity to keep up with the ever-changing environment of the Internet.

Worse, policy makers continue to think of the Internet as just another tool—sort of like a telephone, but quicker. But the things that "everybody knows" are changing every day. Until we come to grips with the ubiquity and rapidity of the Internet and the fundamental way in which the Internet creates asymmetries that empower the individual to the disadvantage of the nation-state, we won't really build good cyber policy. It's a daunting task—but no easier for putting off to the future.