September 25, 2011

Cyberthreats And The Limits Of Bureaucratic Control

Susan Brenner

CYBER-THREATS AND THE LIMITS OF BUREAUCRATIC CONTROL

BY

SUSAN W. BRENNER

TABLE OF CONTENTS

I. Introduction

> *[The] bureaucratic type of administrative organization is . . . capable of attaining the highest degree of efficiency*.[1]

For over half a decade, I have been writing about how, and why, the institutions on which modern nation-states have relied to fend off the threats -- war, crime and terrorism – that can erode their ability to maintain order and compromise their viability as sovereign entities become ineffective when the threats migrate into cyberspace. In a succession of law review articles and books, I refined my analysis of the essentially unprecedented challenges cybercrime, cyberterrorism and cyberwarfare pose for law enforcement and the military. In § II of this article, I review that analysis, outlining the nature, causes and likely consequences of those challenges if they are left unchecked

My goal here is to take this analysis to the next level: to go beyond critiquing the efficacy of the current threat-control structures[2] and outline an alternative approach. I am, of course, not the first to make such an attempt. As I explain in § III, law-makers, law-enforcers and military personnel in various countries have proposed and/or are in the process of implementing measures that are designed to modify the existing threat-control structures so as to improve their efficacy against cyber-threats.

Section III's description of these undertakings focuses primarily on efforts in the United States, for two reasons. One is that I am more familiar with U.S. law and U.S. threat-control structures than I am with their correlates in other countries.[3] The other reason is that the United States' arsenal of threat-control structures is larger and more complex than the arsenals of most, if not all, countries,[4] which inferentially suggests

---

[1]Max Weber, The Theory of Social and Economic Organization 337 (T. Parsons, ed,, trans. A. Henderson & T. Parsons 1947).

[2]I use the phrase "threat-control structures" to denote the institutional arrangements a society relies upon to keep the threats that can erode social order and undermine its viability in check. As I note above, the threats traditionally consisted of crime, terrorism and war; as I explain in § II, they now also include cyber-variants of each threat, i.e., cybercrime, cyberterrorism and cyberwarfare. As § II also explains, the threat-control structures contemporary societies rely on for this purpose so far consist of law enforcement agencies and personnel plus military agencies and personnel.

[3]And, like most Americans, my only language is English, which means I find it difficult to access existing and proposed legislation in most non-English speaking countries.

[4]As to the complex structure of the United States' threat-control initiatives, *see, e.g.,* US Homeland Security & Defense Structure, Homeland Security Research, http://www.homelandsecurityresearch.com/wp-content/uploads/2009/12/US-HLS-HLD-Structure-2010.pdf. This chart only displays the federal agencies that are involved in the United States' threat-response and –control effort. As such, it encompasses both law enforcement and military agencies, as well as agencies that engage in threat-control activities but do not fall neatly into either category, e.g., the Central Intelligence Agency

and National Security Agency. Sections II and IV review the challenges a bifurcated threat response structure create with regard to cyber-threat-response and –control.

In illustrating the relative difference in the size of U.S. threat-response entities, I will focus only on law enforcement personnel; while military personnel can, and do, play a role in addressing cyberwarfare, at the least, the number of military personnel involved in this effort is limited, relative to the total number of military personnel. *Compare* Army Cyber Unit Expands as Fast as It Can, Defense Systems (February 25, 2011), http://defensesystems.com/articles/2011/02/28/cyber-defense-army-cyber-command.aspx (headquarters of United States' new Cyber Command will "have a staff of more than 1,000 people when it is complete") *with* Active Duty Military Personnel Strengths by Regional Area and By Country (September 30, 2010), U.S. Department of Defense, http://siadapp.dmdc.osd.mil/personnel/MILITARY/history/hst1009.pdf.

As to the size of U.S. law enforcement, *see, e.g.,* Local Police Departments 2007 6, U.S. Department of Justice – Bureau of Justice Statistics (December 2010), http://bjs.ojp.usdoj.gov/content/pub/pdf/lpd07.pdf (in 2007, the "estimated 12,575 local police departments operating in the United States . . . employed approximately 463,000 full-time sworn personnel" plus "about 138,000" full-time civilian employees); Sheriff's Offices, U.S. Department of Justice, Bureau of Justice Statistics, http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=72 (in 2004, 3,067 sheriffs' offices "had an estimated 330,274 employees"). A 2004 survey showed that the 49 "[p]rimary [s]tate" law enforcement agencies, e.g., highway patrol, state troopers, had 89,265 full-time employees and 708 part-time employees. *See* Census of State and Local Law Enforcement Agencies, 2004 2, U.S. Department of Justice, Bureau of Justice Statistics, http://bjs.ojp.usdoj.gov/content/pub/pdf/csllea04.pdf. And another, roughly 60,000 officers were engaged in law enforcement at the federal level. *See* Federal Law Enforcement Officers, 2004, Bureau of Justice Statistics Bulletin 2 (July 2006), http://bjs.ojp.usdoj.gov/content/pub/pdf/fleo04.pdf. From these, somewhat dated, reports, it seems fair to estimate that state and local law enforcement agencies in the United States employ over three-quarters of a million people.

Compare that with the number of police in many countries. *See, e.g.,* Police Officers, Eurostat (November 29, 2010), http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=crim_plce&lang=en#; Sworn Police Offices in Australia, Australian Institute of Criminology (February 2006), http://www.aic.gov.au/publications/current%20series/cfi/101-120/cfi116.aspx (45,201 full-time police officers in Australia in 2204-2005). *But see* China to Unify Police Identity Card from Jan. 1, China.org.cn (January 1, 2007), http://china.org.cn/english/news/194799.htm (China then had "1.6 million police officers").

As to complexity, the United States' federal structure means the responsibility for law enforcement is shared by and/or parsed out among a series of state, local and federal agencies. *See, e.g.,* Paul Mysliwiec, *The Federal Death Penalty as a Safety Valve,* 17 Va. J. Soc. Pol'y & L. 257, 262 (2010) ("in our system of dual sovereignty, the federal criminal code exists parallel to the criminal codes of the . . . states, and . . . there is a great deal of overlap"). Many countries have a national police agency, which reduces, if it does not eliminate, problems resulting from overlapping jurisdiction. *See, e.g.,* James B. Jacobs & Dimitra Blitsa, *Sharing Criminal Records: The United States, the European Union and Interpol Compared,* 30 Loy. L.A. Int'l & Comp. L. Rev. 125, 183 (2008) ("EU

that the challenges it faces are likely to be more intractable than those other countries confront.[5] In other words, what is true for the United States is likely to be true for other countries, as well.[6]

---

nations usually have a single national police department that has authority over local units throughout the country"). *See also* "National Police Agency (Republic of Korea)," Wikipedia, http://en.wikipedia.org/wiki/National_Police_Agency_(Republic_of_Korea); The Ministry of Public Security of the People's Republic of China, http://big5.mps.gov.cn/SuniT/www.mps.gov.cn/English/index.htm. And, as § III notes, most countries do not have the rigid bifurcation between law enforcement and military initiatives that is found in the United States.

[5]As James Q. Wilson noted in his study of bureaucracy, government agencies "view any interagency agreement as a threat to their autonomy." James Q. Wilson, Bureaucracy: What Government Agencies Do and Why They Do It 192 (2000). He also pointed out that the "chief result of the [bureaucratic] concern for turf . . . is that it is extraordinarily difficult to coordinate the work of different agencies." *Id.* Wilson notes that business bureaucracies "coordinate their actions by responding to market signals" and, where appropriate, by "entering into explicit agreements . . . in which mutual material gain is the criterion for cooperation." *Id.* "Government agencies, by contrast, view any interagency agreement as a threat to their autonomy." *Id.* They also "resist being regulated by other agencies." *Id.* at 193.

Given all that, it is not surprising that many of the challenges noted above arise from competition among agencies. *See, e.g.,* Richard A. Martin, *Book Review: Cops Across Borders: The Internationalization of U.S. Criminal law Enforcement*, 18 Fordham Int'l L.J. 368, 374 (1994):

> `Turf battles,' which often exist between law enforcement agencies in the United States, become even more complicated overseas because the number of agencies with potential jurisdiction over any particular crime is much greater, and the goals of those agencies are often diverse. Thus, while a particular crime might be investigated in the United States by the Federal Bureau of Investigation, the Drug Enforcement Agency (`DEA'), the Customs Service, and local authorities, overseas the same crime might also be investigated by the Department of State, the Central Intelligence Agency, and the military investigative services (the Naval Investigative Service, the Air Force Office of Special Investigations, and the Military Police). Indeed, any incident involving attacks on American citizens or American property is often the subject of overlapping investigations by U.S. State and Defense Department units, as well as traditional law enforcement agencies of the U.S. Department of Justice. The problems which derive from the different goals of the agencies . . . present a continuing dilemma that the United States has not resolved.

(note omitted). The author's observations on the turf battles that arose in 1990s drug investigations apply with at least equal force to cybercrime investigations. *See, e.g.,* Jeffrey Hunker, *Editorial,* Pittsburgh Post-Gazette B1 (June 7, 2009), 2009 WLNR 10912567:

> [O]ur efforts get muddled in an alphabet soup of agencies and plans. Agencies responsible for pursuing cyber crime -- just one aspect of cyber security -- include the Secret Service, the FBI, the Federal Trade Commission and a special office in the Justice Department. Meanwhile the National Security Agency has been fighting a turf battle with the Department of Homeland Security over who should `run' the nation's cyber-security efforts.

See also Bruce Reed and Marc Dunkelman, *Policing Our Cyberstreets,* Boston Globe 13 (October 21, 2009), 2009 WLNR 20771921 (noting that in dealing with "cybercrime and cyberterrorism, competition and turf wars between bureaucracies . . . frequently stymie the implementation of workable solutions"). And the author of the editorial quoted above focuses only on *federal* agencies that are responsible for cybercrime and cybersecurity. *See* Jeffrey Hunker, *Editorial,* Pittsburgh Post-Gazette B1, *supra.* But the "alphabet soup" of agencies involved in investigating cyber attacks also includes officers from state and local law enforcement agencies noted above, which further intensifies the competition in this area. *See supra* note 4. *See, e.g.,* Ryan J. Reilly, *Federal Agents Say Turf Wars Have Negatively Affected Investigations,* TPM (May 9, 2011), http://tpmmuckraker.talkingpointsmemo.com/2011/05/federal_agents_say_turf_wars_have_negatively_affec.php; Richard J. Brennan, *Border Security in Spotlight as Harper Goes to Washington,* Toronto Star A17 (February 2, 2011), 2011 WLNR 2071213; Richard A. Martin, *Book Review: Cops Across Borders,* 18 Fordham Int'l L.J. 468, 474 (1994).

For a recent example of how inter-agency rivalries undermine the U.S. response to cyber-threats, *see, e.g.,* U.S. Department of Justice, - Office of the Inspector General The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat iv, 12-13 (April 2011), http://www.justice.gov/oig/reports/FBI/a1122r.pdf (noting FBI's failure to share threat information with other law enforcement agencies). The 9/11 attacks were unintentionally facilitated by a similar lack of information-sharing. *See, e.g.,* Thomas H. Kean & Lee H. Hamilton, 9/11 Commission Report 78-80, 88-89, 91-92 355-356 http://www.gpoaccess.gov/911/pdf/fullreport.pdf (2004). For a summary of how and why information-sharing failed in the lead-up to the 9/11 attacks, *see* James B. Perrine, Verne H. Speirs & Jonah J. Horwitz, *Fusion Centers and the Fourth Amendment: Application of the Exclusionary Rule in the Post-9/11 Age of Information Sharing,* 38 Cap. U. L. Rev. 721, 729 (2010).

And for an analysis of how, and why, inter-agency lack of cooperation continues to impede intelligence collection and analysis in the post-9/11 world, *see* Steven K. O'Hern, The Intelligence Wars: Lessons from Baghdad 207-256 (2008). Among other things, O'Hern notes that bureaucracies' tendency to develop "stovepipes" impedes information-sharing and cooperation among agencies:

> The term `stovepipe' refers to the lack of sharing among intelligence organizations. In a stovepipe, intelligence is collected by an organization, analyzed by the same organization, and passed up the chain to that organization's higher headquarters – but not shared outside of the organization.

As § III explains, these proposals appropriately focus on remediating specific factors that contribute to the inefficacy with which current U.S. threat-control structures confront cyber-threats. As I explain in § IV, such an approach is inadequate because it seeks to "update" systems that were developed to control threats that were simpler and more parochial than the ones we confront now. I do not believe our existing threat-control structures can be modified in ways that will make them effective against the twenty-first century threats many countries already confront, and most, if not all, will eventually confront.

Like others, I believe we need a new threat-control strategy: One that replaces the rigid, hierarchical structures on which we currently rely with systems that mirror the

---

Id. at 211-212. He notes that stovepipes develop "for many reasons", perhaps the most important of which is that people work for "different organizations that have different missions", which can lead to a failure to share information "out of hubris". *Id. at* 213, 227. As to the latter, O'Hern explains that the hubris arises because people believe their organization "can do more with the information" than could be done if they share it with other organizations. *Id.* at 227.

Finally, as many have noted, bureaucracies are by nature risk-averse. *See, e.g.,* James Q. Wilson, Bureaucracy: What Government Agencies Do and Why They Do It, *supra* at 69 ("government organizations are especially risk averse because they are caught up in a web of constraints so complex that any change is likely to rouse the ire of some important constituency"). It is therefore not surprising that agencies often suffer from a failure of ambition. *See, e.g.,* Thomas H. Kean & Lee H. Hamilton, 911 Commission Report 352 http://www.gpoaccess.gov/911/pdf/fullreport.pdf (2004):

> Government agencies . . . sometimes display a tendency to match capabilities to mission by defining away the hardest part of their job. They are often passive, accepting what are viewed as givens, including that efforts to identify and fix glaring vulnerabilities to dangerous threats would be costly, too controversial, or too disruptive.

See also Ralph Peters, Beyond Terror: Strategy in a Changing World 197 (2002) ("[B]ureaucracies discourage risk-taking . . . that does not match the models of the past. The motto . . . is `Play it safe'").

[6]For now and for the currently foreseeable future, this is most likely to be true for countries that (i) are frequent targets of cyberattacks and (ii) rely on the hierarchical response structures examined in § II, *infra*. As to the first factor, *see, e.g.,* Trend Micro, The Business of Cybercrime: A Complex Business Model 2 (January 2010), http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/wp04_cybercrime_1003017us.pdf ("U.S. and Western Europe are popular targets"). *See also* Matt Liebowitz, *"Oddjob" Trojan Sneaks into Your Bank Account,* MSNBC (March 14, 2011), http://www.msnbc.msn.com/id/41743730/ns/technology_and_science-security/t/oddjob-trojan-sneaks-your-bank-account/ (cybercriminals attacking targets "in the United States, Poland and Demark").

lateral, networked structures that prosper in cyberspace.[7] In § V, I outline my thoughts as to how such a strategy could be structured and implemented.

II. Threats

As § III explains, cybercrime, cyberterrorism and cyberwar differ from their real-world analogues in various ways, which means that strategies devised to deal with the former may not be effectual in dealing with cyber-threats. To understand why that is true, it is necessary to understand the distinctions between the traditional threat categories -- crime, terrorism and warfare -- and how cyberspace erodes those distinctions.[8] This section addresses those issues.

A. Real-space

Crime, terrorism and war and the distinctions between each are reasonably well defined and reasonably stable in the physical world. The definitional clarity and empirical stability of the real-world threat categories is a function of two circumstances: One is that the categories evolved as pragmatic responses to the challenges territorially-based sovereign entities (e.g., city-states, empires, nation-states) must confront and overcome

---

[7]As to the non-hierarchical nature of cyber-threats, *See, e.g.,* Jonathan A. Ophardt, *Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield*, 2010 Duke L. & Tech. Rev, 3, 39 (2010):

> Few, if any, cyber attacks occur in organizations with a formalized chain of command. Instead, multiple members of an organization . . . create a cyberattack capability which is implemented on the decision of potentially different members. The system lacks a true hierarchy of decision making. . . .

See also Testimony of Joe Pasqua before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, Hearing Online Privacy, Social Networking, and Crime Victimization (July 28, 2010), 2010 WLNR 15174513 (2010) (cybercriminals "range from loose collections of individuals to organized and sophisticated groups"); Henry Reed, *Enterprise Threat and Monitoring Delivers the Rewards without the Risk,* 4/1/10 Database and Network J. 18, 2010 WLNR 11316176 (2010) (a "loosely-coupled and . . . well-organised group of players a cyber criminal can attack any size institution"). As to why hierarchical structures are not effective in dealing with cyber-threats, *see, e.g.,* Clay Wilson, Botnets Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress CRS-30 (November 15, 2007), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA474929 (online activity "requires less personal contact, less need for formal organization, and no need for control over a geographical territory", all of which mean that online crime will tend to "emphasize lateral relationships and networks instead of hierarchies").

[8]For more on the traditional threat categories, *see* Susan W. Brenner, Cyber-threats: The Emerging Fault Lines of the Nation-State 13-23 (2009). *See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security,* 10 B.U. J. Sci. & Tech. L. 1, 5-64 (2004).

if they are to survive.[9] The other circumstance is the fact that these threats emerged in a physical environment that is far less malleable and therefore far less ambiguous than the conceptual environment of cyberspace.[10]

Probably the greatest challenge societies confront is the need to maintain order, both internally and externally.[11] Order is essential if the citizens of a society are to carry out the functions (e.g., procure food and shelter, reproduce) essential to ensure their survival and that of the society.[12] As failed states demonstrate, a society cannot survive if its members are free to prey on each other in ways that undermines the level of order needed to maintain a functioning society.[13] To maintain order internally, a society must ensure that its citizens are organized and socialized in a fashion that lets them carry out essential functions and that this internal order is not undermined by the disruptive activity of some citizens.[14] To maintain order externally, a society must fend off encroachments and attacks by other societies.[15] To do this, a society must have trained personnel who are equipped with the weaponry they need to repel external attacks.[16]

1. Rules

Societies use two sets of rules to maintain internal order.[17] One consists of civil rules that define the basic structure of the society. These rules deal with status (e.g., when people become adults, which adults have which rights), property (e.g., who can own property, how one acquires property), familial bonds (e.g., kinship, marriage,

---

[9]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 34-46. For a summary of the characteristics of the modern nation-state, *see* Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 156.

[10]*See, e.g., id.* at 50-53.

[11]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 34-46. at 9-11.

[12]*See id.*

[13]*See, e.g.,* Daniel Thürer, *The "Failed State" and International Law,* 836 International Review of the Red Cross 731 (1999), http://www.icrc.org/web/eng/siteeng0.nsf/iwpList175/438B7C44BDEAC7A3C1256B66005DCAAB.

[14]*See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 9-11.

[15]*See id.*

[16]In other words, the state monopolizes the use of force in order to control threats that can disrupt order. *See, e.g.,* Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 156.

[17]The discussion in this section is taken from Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 9-60.

divorce) and other equally critical matters. Many civil rules are informal norms; most citizens internalize the norms and that keeps their behavior within socially acceptable bounds. Other civil rules take the form of laws, the enforcement of which falls to civil courts and civil litigation (suits between individuals).

Unlike other social species (e.g., ants, termites), humans are intelligent and can therefore deliberately decide not to follow a rule. Most of the individuals in a society will not intentionally disobey the society's civil rules, but some will. Societies use a second set of rules -- criminal rules -- to control conduct that deliberately violates a society's rules and challenges its ability to maintain order. These rules are intended to discourage rule-violation by letting the state sanction those who commit "crimes."

A crime consists of violating a rule – a law -- that prohibits certain conduct or causing certain "harm." Murder, for example, prohibits causing the death of another human being; theft prohibits someone's taking another person's property without her permission and with the intention to deprive her of it. As these examples indicate, criminal rules often relate to matters governed by civil rules; the prohibition against theft reinforces civil rules that establish and define the parameters of property ownership.

Criminal rules discourage rule violations by proscribing certain activity and by prescribing and inflicting sanctions on those who engage in it. So if Jane murders John, the society they belong to will convict her of murder and impose a sanction. The primary purpose of sanctioning offenders is to deter them from breaking more criminal rules; a secondary goal is to deter others from following their example. That presumably deters enough would-be rule-violators to keep crime from undermining order in that society.[18]

This system assumes individuals commit crimes.[19] That assumption also applies to terrorism, which consists of committing what would otherwise be routine crime(s) for ideological reasons.[20] Criminals commit crimes for financial reasons (e.g., fraud, theft) or passion (e.g., anger, sex).[21] The motive for committing crimes is personal: I steal to benefit myself; I murder out of revenge. Terrorists commit crimes (e.g., killing people,

---

[18]*See, e.g.,* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime,* 23 J. Marshall J. Computer & Info. L. 659, 662 (2005) ("societies accept that they cannot eliminate it and so strive to control it.").

[19]*See, e.g.,* Jaya Ramji-Nogales, *Designing Bespoke Transitional Justice: A Pluralist Process Approach,* 32 Mich. J. Int'l L. 1, 6 (2010). This assumption derives from the fact that, until recently, humans were the only "persons" whose actions were recognized and governed by law. *See, e.g.,* Anonymous Case (No. 935), 88 Eng. Rep. 1518, 1518 (K.B. 1701) ("corporation is not indictable but the particular members of it are"). And so far, they seem to be the only "persons" who are committing cybercrimes and/or seem likely to commit cyberterrorism or engage in cyberwarfare.

[20]See*, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare,* 97 J. Crim. L. & Criminology 379, 386-389 (2007).

[21]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 57 n. 331.

damaging property) to promote an ideology.[22] Since terrorists commit crimes (albeit for distinct motives), societies have historically regarded terrorism as a type of crime.[23]

2. Territory

Historically, crime and terrorism were an internal phenomenon, i.e., both were committed within the territory of a sovereign entity,[24] such as a nation-state.[25] The internal character of crime/terrorism was a function of necessity: In the real-world, it is physically impossible for me to steal property from someone in another country; the constraints of geography and historic limitations of travel meant crime and terrorism were domestic threats which could be addressed with local law and local law enforcement agencies.[26]

War differs from crime and terrorism in two respects, one of which is that it is a struggle between sovereign entities.[27] While individuals wage war, warriors are merely implements; the players are the nation-states engaged in a political struggle.[28] War has been reserved for sovereign entities because only they could summon the resources (manpower, weapons) needed to wage war.[29] Historically, individuals engaged in crime and terrorism and nation-states engaged in war. Each category was distinct: individuals did not "commit" war and sovereign entities did not "commit" crime or terrorism.[30] The second respect in which war differs from crime/terrorism is that war threatens a society's ability to maintain external order -- to fend off attacks from hostile states and maintain the stable geographical and political environment essential for its survival.[31] War has historically been an "outside" threat; crime and terrorism have been an "inside" threat.[32]

---

[22]*See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 20 at 386-389.

[23]*See id.* at 386 n. 40.

[24]For the link between territory and sovereignty, *see, e.g.,* For a summary of the characteristics of the modern nation-state, *see* Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 156 (nation-states is "a compulsory association with a territorial basis").

[25]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 48.

[26]*See id.* at 39-56.

[27]*See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 22 at 402-404.

[28]*See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts,* 43 Vand. J. Transnat'l L. 1011, 1023 (2010).

[29]*See* Susan W. Brenner, Cyber Threats, *supra* note 8 at 15-17.

[30]*See id.* at 15-23.

[31]*See id.*

We saw above how societies developed rules that define crime and terrorism. They also eventually developed rules that defined war and set certain parameters on how it is to be conducted.[33] These rules became the foundation of a strategy that has been effective in controlling real-space threats.[34] But as the sections below explain, the rules and their enforcement both become problematic as threat activity migrates online.

B. Cyberspace

Cyberspace introduces a new variable into the threat-control calculus. As is explained below, by allowing activity to be vectored through non-physical "space," it creates opportunities for conduct that threatens a state's ability to maintain internal and/or external order but (i) does not fit within the traditional threat taxonomy and (ii) diminishes the effectiveness of the systems designed to control those threats.

1. Internal Threats

Cyberspace's most significant contribution to the evolving state of affairs noted above is that it eliminates the constraints of the physical world and makes geography irrelevant: Cybercriminals can attack victims in other countries as easily as they can target someone in their neighborhood.[35] And while we may not as yet seen a verified incident of cyberterrorism, the same will be true of it as well.[36] This means cybercrime and cyberterrorism can be internal threats, external threats or a combination of both. It also means that it can be difficult or even impossible to accurate categorize an attack as cybercrime, cyberterrorism or cyberwarfare.[37]

Cyberspace also vitiates identity: Cybercriminals and/or cyberterrorists can be anonymous or assume false identities with an efficacy that is impossible in the physical world, where one's physical characteristics limit the number and nature of identities he or

---

[32]*See id.*

[33]*See, e.g.,* David Weissbrodt & Daniel H. Nesbitt, *The Role of the United States Supreme Court in Interpreting and Developing Humanitarian Law,* 95 Minn. L. Rev. 1339, 1372-1373 (2011).

[34]Control is all societies strive for. *See* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime,* 23 J. Marshall J. Computer & Info. L. 659, 662 (2005).

[35]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 69.

[36]*See, e.g.,* Clay Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress CRS-7 to CRS-9, Congressional Research Service (updated January 29, 2008), http://www.fas.org/sgp/crs/terror/RL32114.pdf (2007 Estonia attack).

[37]*See, e.g., id.*

she can assume.[38] The elimination of physical constraints and the masking or alteration of one's identity combine to erode the efficacy of the traditional law enforcement model, which nation-states use to enforce their criminal laws.[39]

The model is based on the premise that societies can maintain internal order by having law enforcement officers react to completed crimes and/or acts of terrorism.[40] It assumes police will apprehend the perpetrators, who are charged, tried and sanctioned; this, as noted above, is presumed to control crime by discouraging the perpetrators and others from following their example.

Since it evolved to deal with crime, which is subject to the physical constraints of the real-world, this model assumes local crime, local perpetrators and a physical crime scene.[41] Police officers use these characteristics of crime to identify and apprehend perpetrators; as we all know, it is exceedingly difficult to commit a physical crime without leaving trace evidence at the scene (and perhaps being observed by witnesses).[42] The officers investigating a crime can also focus on links between the victim and perpetrator because it is equally difficult to mask our movements and relationships in the physical world. These investigative procedures, and the assumptions that underlie them, become problematic when criminal activity is mediated through the cyberworld. [43]

The model's efficacy is further eroded by a third characteristic of cybercrime and cyberterrorism: Since crime and terrorism can be automated, perpetrators can cause "harm" on a scale that surpasses what is possible in the real-world.[44] The increase in the scale of the "harm" inflicted challenges the model because of the sheer number of new crimes and because they constitute a new quantum of criminal activity that is added to the real-world crime with which law enforcement must continue to deal.[45]

2. External Threats

---

[38]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 65-66 & 68-70.

[39]*See id.* at 75.

[40]*See id.* at 58-65.

[41]*See id.* at 50-75.

[42]*See id.*

[43]*See id.*

[44]*See id.* at 50-51, 66-68. *See, e.g.,* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe,* Wired (August 21, 2007), http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1.

[45]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 66-68.

War is unambiguous in the physical world; when the Japanese attacked Pearl Harbor, there was no doubt this was war.[46] The attackers wore uniforms and used airplanes and ships, all of which displayed Japan's national insignia; this was one indicator of war (attack by a nation-state, not individuals).[47] Another indicator was the weaponry itself, which was far beyond the capacity of individuals to acquire and utilize.[48]

We may, or may not, have seen instances of cyberwarfare.[49] We know, though, that it will not require the use of sophisticated, expensive weapons that can only be utilized by nation-states.[50] Like cybercrime and cyberterrorism, cyberwarfare will involve the use of hardware and software that are available to anyone with a computer, Internet access and the requisite computer expertise.[51]

All these factors erode the assumptions on which the three threat categories are based. A cyberattack that comes/seems to come from outside a nation-state's territory and is directed at what would be considered military targets *might* be cyberwar, but it might be cybercrime or cyberterrorism. In cyberspace, states lose their monopoly on war and individuals lose their monopoly on crime and terrorism.

This creates serious problems for countries like the United States, which rigidly bifurcate threat response authority into (i) civilian (crime/terrorism) and (ii) military (war).[52] The bifurcation is predicated on the assumption that response personnel can easily distinguish crime/terrorism from war.[53] That premise is valid in the physical world, but, as explained below, is problematic for conduct vectored through cyberspace.

C. Cyberspace and Threat Response

---

[46]*See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 22 at 406.

[47]*See id.*

[48]*See* Susan W. Brenner*, Cyber Threats, supra* note **Error! Bookmark not defined.** at 75.

[49]*See, e.g.,* Clay Wilson, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, *supra* note 36 at CRS-7 to CRS-9. *But see* Susan W. Brenner*, Cyber Threats, supra* note 8 at 85-94.

[50]*See generally id.* at 75 (weaponry used in kinetic warfare).

[51]*See, e.g.,* Lieutenant Colonel Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. Rev. 43, 59-60 (2009).

[52]*See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 22 at 441-455.

[53]*See id.*

This section explains why the traditional threat categories morph and blur in cyberspace and shows how the erosion of these categories undermines the viability of the bifurcated response strategy outlined above. As this section explains, the strategy implicitly assumes that would-be responders can accurately and confidently carry out the process of attribution, which has been the first step in attack-response,

The concept of attribution is an explicit element of the laws of war,[54] and it is implicit in the laws governing crime and terrorism.[55] The general concept encompasses two issues: attacker-attribution (Who carried out an attack?) and attack-attribution (What kind of an attack was it?). Each is examined below.

1. Attacker-attribution

Attacker-attribution has historically been less problematic for war than for crime or terrorism.[56] The laws of war require warring states to identify themselves; if a country breaches that obligation, it is generally not difficult to identify the state responsible for an act of war in the real-world. The clothing military attackers wear and the equipment they use display insignia indicating their national affiliation.[57] The language they speak and the location from which an attack is launched can also indicate the country from which it originated; in the real-world, it is relatively easy to determine the physical location from which an attack was launched.[58]

Identifying those responsible for crime is usually much more difficult.[59] Criminals have a strong incentive to avoid identification because it is generally the first step toward being apprehended, convicted, and sanctioned for their misdeeds.[60] Since crime control is essential for maintaining internal order, nation-states have developed a standardized, generally effective approach for identifying those who commit crimes in their territory.

This criminal investigation approach assumes activity in the real-world because until recently, physical reality was the only arena of crime commission. As noted above, this approach focuses on finding physical evidence at a crime scene and/or locating witnesses who saw the perpetrator.[61] It assumes the perpetrator was, and perhaps still is,

---

[54]*See, e.g.,* Matthew Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense,* 32 B.C. Int'l & Comp. L. Rev. 439, 450 (2009).

[55]*See, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare* supra note 22 at 405-429.

[56]*See Susan W. Brenner, Cyber Threats, supra* note **Error! Bookmark not defined.** at 127-131.

[57]*See id.* at 128.

[58]*See id.*

[59]*See id.* at 128-129.

[60]*See id.*

[61]*See id.* at 129-129.

in the local geographical area.[62] If attacker-attribution fails for one crime, officers will assume the attacker remains in the area and will consequently be alert for the possibility that he will re-offend and then be identified. [63]

Attacker-attribution for terrorism is more complicated than attack-attribution for war but less complicated than attack-attribution for crime. [64] While those who carry out a terrorist attack may not identify themselves personally, they often identify themselves as acting on behalf of a terrorist group.[65] If the sponsoring group does not claim credit for an attack, the structure and style of the attack may inferentially identify the organization responsible [66] That may lead investigators to the individuals who carried out an attack. Since the current strategy treats terrorism as a type of crime, the criminal investigation approach outlined above is often used to identify and apprehend individual terrorists.

In analyzing how cyberspace complicates attacker-attribution, it is helpful to employ an example: In 2006, a "sensitive Commerce Department bureau" -- the Bureau of Industry and Security (BIS) -- suffered a debilitating attack on its computer systems."[67] BIS was forced to disconnect its computers from the Internet; it eventually discarded the infected computers and replaced them.[68] The attack was traced to sites hosted by Chinese Internet service providers (ISPs), but the attackers were never identified. [69]

As we saw above, real-world attacker-attribution calculi rely on the "place" where an attack occurred or originated from in determining attacker identity. With virtual attacks, "place" tends to be more ambiguous and less conclusive than in real-world analyses.

(a) Point of attack origin

It is ambiguous because while attacks may be routed through Internet servers located in China, this does not necessarily mean they originated in China. It is common for online attackers to use "stepping stones" – computers owned by innocent parties but

---

[62]*See id.* at 129.

[63]*See id.*

[64]*See id.* at 130.

[65]*See id.*

[66]*See id.*

[67]*See, e.g.,* Alan Sipress, *Computer System Under Attack,* Washington Post (October 6, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/10/05/AR2006100501781.html.

[68]*See id.*

[69]*See id.*

controlled by the attacker – in their assaults.[70] The "stepping stone" computers can be anywhere in the physical world because real-space is irrelevant to activity in cyberspace. So while use of the Chinese servers might mean the attacks came from China, it might not mean that at all. The attacker might be in Russia or Peoria.

What if BIS-style attacks were repeated, with each coming from Chinese servers and targeting computers used by U.S. agencies? Could we base attacker-attribution on inferences drawn from the repetitive use of what seems the same point of origin? It would be risky to rely on mere repetition; aside from anything else, a virtual Machiavelli might be "framing" China by routing structurally similar attacks through its real-space.

Repetition coupled with other circumstances might support using point of attack origin inferences to establish attacker-attribution. Assume that BIS-style attacks are launched against another U.S. agency's computers. Investigators trace these attacks to servers in Guangdong, China. For two years, sporadic attacks targeting U.S. civilian and government computers have been traced to Guangdong; some say Chinese military hackers conducted the attacks, others say Guangdong University students were responsible. Can we predicate attacker-attribution inferences on the discontinuous repetition of similar target attacks coming from the same real-world locus in China? Does the (reasonably reliable) identification of a single point of origin support the inference that the recent BIS-style attacks came from Guangdong?

For the purposes of analysis, we will assume the facts outlined above support the inference that "someone" in Guangdong launched the hypothesized BIS-style attacks. That raises the next question: how, if at all, does the inference that the attacks came from Guangdong advance the process of identifying who is responsible for them?

(i) War

Point of attack origin historically played an important role in attacker-attribution for acts of war because the targets of such attacks usually inferred an attack originating in another nation-state is attributable to that nation-state.[71] If we apply this logic to the scenario above, the United States could rationally infer that the BIS-style attacks on U.S. government computers were acts of war launched by China. It could, in effect, construe the attacks as the virtual equivalent of Japan's attack on Pearl Harbor. The problem with this derivative inference of responsibility lies in equating an attack inferentially launched *from* Chinese territory with an attack launched *by* China.

Historically, it was reasonable to equate transnational attacks with acts of war because only a nation-state could launch such an attack.[72] That is still true in the real-world, but cyberspace gives each nation-state an incremental, highly permeable set of

---

[70] *See, e.g.,* Jeffrey Hunker, Bob Hutchinson & Jonathan Margulies, *Role and Challenges for Sufficient Cyber-Attack Attribution* 6, Institute for Information Infrastructure Protection (2008), http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

[71] *See Susan W. Brenner, Cyber Threats, supra* note **Error! Bookmark not defined.** at 141-143.

[72] *See id.* at 142.

"virtual" national borders.[73] Anyone with Internet access and certain skills can launch a cross-border virtual attack on the cyberspace "presence" of an external nation-state. A virtual attack is not territorially invasive, but produces effects in the victim-state's territory that are damaging in various ways and in varying degrees. [74]

Point of attack origin therefore plays a more problematic role in analyzing online warfare, which brings us to the role it plays in the crime-terrorism calculus. While crime and terrorism are conceptually distinct, we will consider them jointly because both represent threats to internal order and both are the product of individual actions.

(ii) Crime/terrorism

Point of attack origin historically played a much more limited role in crime and terrorism attacker-attribution than in war attribution.[75] While point of attack origin can inferentially indicate who may have been responsible for a crime or an act of terrorism, the link between origin and attribution is much more attenuated than in war analysis.

The primary reason for this is that in the real-world, point of attack origin and point of attack occurrence are often so closely related as to be indistinguishable for crime, and for terrorism. A crack dealer sells crack in his neighborhood; the points of origin and occurrence of his drug crimes are functionally identical. A terrorist group operating from City A bombs a restaurant in nearby City B; since the points of attack origin and occurrence were separated by only a short distance, one can argue that they are functionally identical here as well. If there is little or no differentiation between the point of attack origin and the point of attack occurrence, identifying the point of origin is unlikely to markedly advance the process of identifying the attacker.

Point of attack origin therefore tends to be one, perhaps minor, factor in the processes law enforcement officers use to identify those responsible for crime and terrorism. It has played a lesser role in crime/terrorism attacker-attribution because these threats to internal order have come primarily, if not exclusively, from domestic actors. Domestic actors are presumptively in the nation-state where the attack occurred, and investigators tend to assume that they remain in the area where it occurred.

As crime and terrorism migrate online, point of attack origin can assume more importance in attacker-attribution. As we saw above, cyberspace eliminates the need for physical proximity between attacker and victim and creates the potential for increased differentiation between point of attack origin and point of occurrence. In other words, it erodes law enforcement's ability to assume an attacker is parochial. The viability of that default assumption still holds for real-world crime, and can hold for real-world terrorism, but its applicability to online crime and terrorism is increasingly problematic.

---

[73] *See id.*

[74] *See, e.g.,* Clay Wilson, Botnets, Cybercrime, and Cyberterrorisms, *supra* note 36 at CRS-7 to CRS-9 (large-scale, sustained online attacks on Estonian infrastructure).

[75] The discussion in this section is taken from *Susan W. Brenner, Cyber Threats, supra* note 8 at 143-161.

The parochial-attacker assumption is most likely to hold for "personal" attacks: cybercrimes and, perhaps, acts of cyberterrorism in which the perpetrator's motives are idiosyncratically emotional. In these cases – e.g., John uses cyberspace to stalk his former girlfriend or Jane uses it to attack her employer – the perpetrator and victim are in the same area, but instead of using physical activity in that real-space to conduct the attack, the perpetrator vectors it through cyberspace.

This creates an epistemological issue: When attacker and attacked are in the same real-space area throughout an attack conducted online, did the attack originate in the real-space occupied by attacker and victim, online or in both? For the purposes of attacker-attribution, the answer should be both.

In "personal" attack cases, the connections between attacker and victim mean the parochial-attacker assumption is likely to be useful in identifying the attacker. So far, cyber-vendettas seem primarily to originate in real-world contacts between attacker and victim. Investigators can therefore rely on the approach used for real-world crime and terrorism, i.e., focus on inferences derived from a real-world context. The attack, then, should be construed as originating in the real-space occupied by attacker and victim.

What about attacks in which the attacker is not, by any definition, in the same real-space as the victim? In the BIS attacks, the target was in Washington, D.C., while the attackers were (presumably) in China. An identified point of attack origin serves a very different function in cases like this, for several reasons.

First, it serves an initial, essentially negative function in attacker-attribution. It tells investigators that the parochial-attacker assumption and derivative investigative approach they use for real-world crime/terrorism will probably be of little use in identifying the attackers. When an attack presents functionally coterminous points of attack origin and occurrence, we have a localized crime scene that becomes the focal point of the investigation. Evidence, inferences, observations of witnesses and connections between victim and attacker all radiate from and revolve around this unitary crime scene. It creates a comprehensible focus for the investigation and, in so doing, makes the investigation a manageable task.

Cyberspace fractures the crime-scene into shards, the number of which depends on the particular circumstances of an attack. One constant shard is the alpha point of attack origin – the place where the attacker is physically located and from which she launches the attack. Other, variable shards are the intermediary points of transmission used in the attack; each represents the occurrence of a constituent, spatially diverse event that contributed to the success of the ultimate attack. The other constant shard, the omega shard, is the place of attack occurrence, which we examine below.

Fracturing the crime scene into shards makes identifying the point of attack origin and linking it to the attacker much more difficult. Aside from anything else, a fractured crime scene can result in false positives – in investigators assuming an intermediary point of transmission of an attack is the originating point for the attack.

Another issue that can complicate the process of backtracking through a series of incremental attack stages is the legal process involved. Incremental attack stages will almost certainly involve the use of computers in different countries. To gain access to the information needed to trace an attack through those computers, law enforcement will

have to obtain assistance from government and civilian entities in the countries in which the computers were used. This process can be difficult, time-consuming and even futile. The formal methods used to obtain assistance can take months or even years; since digital evidence is fragile, it may have disappeared by the time investigators obtain the assistance they need.

Even if investigators obtain the assistance they need and can trace an attack to its point of origin, this may not markedly advance their effort to identify the attacker. Investigators in the BIS case ascertained that the attacks came from servers in China, but this information could neither directly nor inferentially establish who was responsible for the attacks or, indeed, what kind of attacks they were.

In sum, while point of attack origin can play a role in identifying the attackers in a cybercrime or cyberterrorism event, its function tends to be limited, and will probably become more so as cyberattackers become more sophisticated about hiding their tracks.

(b) Point of attack occurrence

For real-world warfare, point of attack occurrence is the essential complement to point of attack origin: Point of attack origin tells us which country initiated war; point of attack occurrence tells us which country is the "victim." [76]

As with point of attack origin, the point of attack occurrence calculus becomes ambiguous when war migrates online. Consider the BIS attacks: They occurred in the United States. What, if anything, does that tell us about who is responsible for them?

We will assume the attacks originated in Guangdong, China. Can we infer that cyberattacks originating in China and occurring in the United States represent acts of war attributable to the Chinese government? Unlike real-world acts of war, we do not have the presence of enemy personnel and armament on U.S. soil. We have only the virtual "presence" of signals, which traveled through cyberspace by routine means, the same means used by civilian and government traffic every second of every day. The signals bear neither state insignia nor other markers of nation-state allegiance. Our only bases for concluding they constitute components of an attack by China are their point of origin, their geographic destination, and the nature of the harm they inflicted (damage to U.S. government computers).

We have already analyzed the ambiguity involved in determining point of attack origin. Here, the point of attack occurrence is not ambiguous; we know it occurred in the United States. The ambiguity lies in the implications of this point of occurrence. In the real-world, the occurrence of an act of war on Nation-State A's territory is equivalent to a declaration of war by the state responsible for the attack because war has historically been about territory. The violation of one nation-state's territorial integrity by agents of another nation-state is a challenge to its ability to maintain external order.

In the real-world, the singular inference to be drawn from an attack originating in the territory of one nation-state and occurring inside the territory of another is war. Real-

[76]The discussion in this section is taken from *Susan W. Brenner, Cyber Threats, supra* note 8 at 156-161.

world transborder attacks have been equated with war because only nation-states could launch such attacks.

Cyberspace changes that: We cannot infer from the mere fact that the attacks targeted computers on U.S. soil that they are the equivalent of Hitler invading Poland. In utilizing point of attack occurrence in attacker-attribution, we must modify the assumption that equates transborder attacks with war so it incorporates a basic reality of the online environment: U.S. government and civilian computers are attacked because they are attractive targets for criminals, terrorists, and, ultimately, perhaps, nation-states bent on war. Since U.S. computers are attractive targets for all three categories of attackers, any of whom can launch transborder attacks, the mere fact an externally-launched attack occurs "in" the United States cannot sustain the conclusion that the attack was an act of war on the part of the nation-state from whose territory it originated.

That brings us to crime/terrorism: Point of attack occurrence is an integral component of attacker-attribution for both. Investigations concentrate on the place where the attack occurred. As noted earlier, this investigative model is based on the assumption that the players in the attack dynamic occupied shared real-space; this assumption derives from the fact that physical proximity is an essential prerequisite for the commission of real-world crime or terrorism.

Thus, point of attack occurrence plays a central role in investigating of these real-world events. It is the most likely source of physical evidence and eyewitness testimony that can be used to identify an attacker and link him to the crime/act of terrorism. The larger spatial context in which the crime scene resides provides a potential source of further testimony and data that can become the basis of inferential linkages between victim and attacker. And the place where the attack occurs is sometimes itself a source of inference as to the identity of an attacker. If someone is murdered in a home with an armed alarm system, this suggests the attacker knew the victim.

Here, again, the importance of point of attack occurrence diminishes as attacks move online. A real-space attacker's gaining entry to a home with an alarm system suggests the attacker knew the victim, but a cyberspace attacker's gaining entry to a computer hooked to a cable modem does not. The physical constraints that govern action in the real-world make it eminently reasonable to draw certain inferences from the place where an attack occurred; the absence of those constraints makes it problematic to predicate similar inferences on the place where a virtual attack occurred. Cyberspace nullifies the influence of the three spatial dimensions that constrain action in the real-world and, in so doing, erodes the significance of place in attacker-attribution.

Point of attack occurrence can still play some role in attacker-attribution for online crimes and terrorism because it is part of a larger crime scene and will therefore contain evidence that can be used in an attempt to track the perpetrator(s). Unlike a real-world crime scene, it is not self-contained; the evidence it contains is part of a sequence of digital evidence that is strewn around cyberspace. Since the point of attack occurrence accounts for only part of the evidence, its role in the process of identifying the attacker is accordingly reduced.

2. Attack-attribution

As noted earlier, attacker-attribution has historically been problematic in the real-world, at least for crime and terrorism, but attack-attribution has not.[77] This is due to the distinction societies have drawn between internal and external threats.

Until relatively recently, the limitations of travel and state monopolization of military-grade weaponry made it functionally impossible for non-state actors to challenge a nation-state's ability to maintain its territorial integrity.[78] External order was a purely sovereign concern; nation-states challenged each other in the international arena and resolved matters with military combat.[79] Non-state actors were limited to challenging a state's ability to maintain internal order, i.e., by committing crimes or acts of terrorism. That changes as activities move online.

(a) Real-space

Crime is easily identified because it involves the civilian-on-civilian infliction of familiar categories of harm, such as theft, murder and arson. And as noted above, it tends to be limited in scale because of the constraints physical reality imposes on action in the real-world. Crime usually involves one-to-one victimization, i.e., one perpetrator and one victim (at a time).[80]

Real-world terrorism is usually easy to identify though it often involves activity that would otherwise constitute crime. Real-world terrorism can usually be distinguished from crime because (i) it seems irrational in that it has no obvious mundane motive, such as self-enrichment or revenge and (ii) the scale on which it is committed often exceeds what we encounter with crime.[81]

Real-world war is even easier to identify: When the Japanese bombed Pearl Harbor, no one who saw the attack could have had the slightest doubt this was war – not crime, nor terrorism. The attackers wore military uniforms featuring Japan's national insignia, flew the Japanese flag, used airplanes and other weapons that were not available to civilians and attacked military targets.[82]

(b) Cyberspace

Our focus is now on identifying the nature of the BIS attacks. We begin by parsing what we know of them: They were deliberate, orchestrated attacks, not computer malfunctions; they targeted U.S. government computers and originated in China, perhaps in Guangdong, which may be associated with China's cyberwar effort.

---

[77] *See supra* § II(C)(1).

[78] *See id.*

[79] *See id.*

[80] *See Susan W. Brenner, Cyber Threats, supra* note 8 at 21, 76.

[81] *See id.* at 40-41, 76.

[82] *See id.* at 74.

The circumstances of the attack suggest it was a sortie into cyberwar. As noted above, historically, an attack originating from one nation-state's territory and terminating on the territory of another presumptively constituted an act of war; that presumption suggests the BIS attacks were war. The validity of that conclusion is reinforced by the fact that the attacks targeted government computers; the nature of the target inferentially supports the premise that the attacks were a foray into cyberwarfare.

While we do not know precisely what the BIS attacks were meant to accomplish, we could logically infer that they were a reconnaissance by China's military, testing the security of U.S. government computer systems. The problem is that we cannot arrive at this conclusion with the requisite level of confidence because the markers we must rely on take on an ambiguity lacking in the real-world. The fact the attacks originated from the territory of another nation-state is a circumstance we can consider, but it carries much less weight than in the real-world, as noted above. The transnational aspect of the attack may, or may not, be significant; the same is true of its originating in Guangdong and targeting computers used by the U.S. government. For years, Guangdong has been producing hackers, and for years civilian hackers of various nationalities have been exploring U.S. government computers. It is as possible that the attacks came from student hackers in Guangdong as it is that they came from the Chinese government.

What if a BIS-style attack targeted a corporate computer system? The nature of the target inferentially suggests it was cybercrime, as we assume criminals attack other civilians. That conclusion would be reinforced if the attackers' actions conformed to what we expect of cybercriminals; if, say, they extracted funds from corporate accounts or personal information from databases. Since we assume civilians are the targets of crime, not war, an attack such as this would almost certainly be construed as cybercrime.

Relying too heavily on this assumption could be a mistake. The attack on our corporate entity could be cyberwar, not cybercrime. China's focus on cyberwar includes attacks on civilian entities. If our default approach to attack-attribution continues to rely on the attacks-on-civilians-are-crime assumption, we will no doubt have a situation in which an act of cyberwarfare is construed as cybercrime.

An analogous, but perhaps less serious, problem arises if the attack on our corporate entity is cyberterrorism. Cyberterrorist attacks are unlikely to be isolated incidents; a cyberterrorist event is more likely to be part of a sequence of attacks that may be separated spatially and/or temporally and that have different points of origin. The attack appears to be cybercrime; and except for serial killers and the odd career robber or serial arsonist, law enforcement is not accustomed to approaching a crime as part of a sequence. This means the response to the components of a sequenced cyberterrorism attack would probably be discrete and isolated; officers in different locations would respond to incidents without realizing they were part of a larger attack.

This problem arises because of our partitioned responsibility for responding to crime/terrorism versus warfare and because we tend to assume crime is a localized phenomenon. A subsidiary factor contributing to the problem is that the markers we rely on to differentiate crime/terrorism from war in the real-world are absent or unreliable when it comes to virtual attacks. In the real-world, we rely on three markers to determine the nature of an attack, two of which we have already discussed: (i) point of attack origin, (ii) point of attack occurrence, and (ii) motive for an attack.

As we have seen, the utility of the first two markers erodes as attacks migrate online. The same is also true, but in a different way and for different reasons, for the third factor. Technology enhances our ability to inflict harm, but does not alter the human psyche; unless and until technology transforms us into cyborgs or some other variety of post-human life, it is reasonable to assume the motives that have historically driven us to inflict harm will continue to account for our doing so, on- or offline. Motive is and will continue to be a valid differentiating factor for cyberattacks: profit drives most crime; ideology drives terrorism; and nation-state rivalries have historically driven warfare. The difficulty arises not with our ability to rely on established motivations as a "marker" that inferentially indicates the nature of an attack. It arises instead with our ability to ascertain the motive behind a specific attack.

We know what the BIS attackers did, but cannot ascertain why they did it. This is likely to be true for many future attacks, as well: while the motive behind what are almost certainly routine cybercrime incidents is usually apparent (e.g., greed, revenge), that may not always be true. Terrorists, for example, are increasingly using cybercrime to finance their real-world efforts, which give us a mixed-motive scenario: The motive for committing cybercrimes is profit, a criminal motive; but the motive for obtaining the profit is to engage in acts of terrorism, a non-criminal motive. It is also increasingly possible that non-state actors could commit cybercrimes to obtain the money needed to launch cyberattacks on a nation-state.

D. Implications

Nation-states control internal threats by adopting laws that proscribe certain behaviors ("crimes") and imposing sanctions on those who engage in such behaviors. And, as we saw above, they use a similar strategy to control external threats: Nation-states arm themselves in an effort to discourage other nation-states from attacking them; and they use their military might to repel attacks, if and when they are launched.

The efficacy of both strategies depends on a state's ability to respond effectively to a threat.[83] Responding requires that a state be able to (i) identify the nature of the threat and (ii) implement measures designed to resolve it as efficiently and effectively as possible. As noted above, many countries – particularly the United States -- use a bifurcated response system: Law enforcement responds (only) to internal threats (crime or terrorism); the military responds (only) to external threats (war).[84] The bifurcation is a function both of pragmatism (e.g., military weaponry is generally unsuited for civilian law enforcement purposes) and policy (e.g., a bifurcated system is considered to be a mainstay of democracy).[85]

---

[83]The discussion of threat response tactics is taken from *Susan W. Brenner, Cyber Threats, supra* note 8 at 163-199.

[84]*See id.* at 164-176.

[85]*See, e.g.,* Daniella Ashkenazy, The Military in the Service of Society and Democracy: The Challenge of the Dual-Role Military 4-5 (1994). *But see* Diana Cecelia Weber, *Warrior Cops: The Ominous Growth of Paramilitarism in American Police Departments,* CATO Institute Briefing Paper No. 50 (August 26, 1999) (the war on drugs encouraged the "militarization of law enforcement in America").

Historically, bifurcating response processes was not a problematic strategy because internal and external threats are readily distinguishable in the physical world. Once a state determined the nature of a threat (internal or external), it took steps to resolve it and prevent the occurrence of other, similar threats. Bifurcated response processes become problematic as threats move into cyberspace because they assume that law enforcement officers or military personnel can easily determine whether a threat is internal or external. As we have seen, that assumption breaks down as threat activity moves into cyberspace because the threat categories (and attendant threat identification processes) assume conduct in the physical world.

As state and non-state threat entities increasingly utilize cyberspace in their attacks, it becomes increasingly difficult to differentiate crime, terrorism and warfare. As we saw above, the indicators traditionally used to identify the various types of attacks become less reliable as attacks migrate into cyberspace because they assume activity in the real-world. If potential responders cannot reliably ascertain the nature of a threat, they may not respond to it, may not respond soon enough or may respond when they should not. In other words, the ambiguity of online threat activity not only erodes our ability to identify threats, it also erodes our ability to respond to them.

Assume, for example, that FBI agents discover an ongoing, BIS-style attack on the computer system used by another federal agency -- the air traffic control system, say. The agents conclude the attacks are coming from a location in China that is associated both with China's military preparation for cyberwar and with university student hackers. If the attacks are cybercrime or cyberterrorism, the FBI can and must respond to them.[86] If they constitute war, the U.S. military must respond.[87]

---

[86]As noted earlier, law enforcement's response to cybercrime and cyberterrorism is usually *ex post*, i.e., officers apprehend the perpetrators, who are arrested, prosecuted, convicted and punished. The FBI can pursue this strategy if it is confident that the attacks are cybercrime or cyberterrorism, but it might not want to wait until the attacks culminate in the infliction of massive harm on U.S. targets. It might want to intervene, just as FBI agents intervene when they encounter a real-world crime in process.

FBI agents might try to block the attacks by shutting down or sealing off the computer systems they target, but if the target is the air traffic control system, that solution might prove more harmful than the attacks. If we assume the FBI could somehow launch a counterattack that would block the incoming attack signals or attack and incapacitate the computers from which they originate, we would then have to determine if such a tactic was lawful under U.S. and international law.

If the targeted computers were in China, the FBI would essentially have created a mirror image of the scenario with which the FBI agents are dealing. That is, computers in China would be coming under attack from signals originating in the United States, more precisely, from a federal government agency's computers in the United States. One downside of this tactic, then, is that it could give rise to more or less credible claims by China that the United States had launched cyberwarfare attacks against that country.

Another, alternative downside is that if the FBI were to block the signals and/or attack the computers from which they originate, this would constitute a crime under Chinese

Given the nature of the attacks and the potential harm involved if they continue, the FBI has little time in which to decide whether they are crime/terrorism or war. The FBI utilizes the analysis examined above, i.e., they consider the place from which the attacks originate, the place where they occur and the motive. The FBI is fairly certain the attacks originate in China, but cannot rule out the possibility they originate elsewhere and are merely being routed through China. The FBI is certain that the attacks target a U.S. government agency and, in so doing, threaten serious harm to U.S. civilians.

FBI agents cannot ascertain the motive for the attack with any certainty; there has been no extortion demand, which could indicate the attacks are not cybercrime. The FBI cannot link the circumstances of the attacks or the apparent sources of the attacks to known terrorist groups or to the Chinese government. The FBI therefore has neither direct nor inferential evidence indicating the attacks are cyberterrorism or cybercrime. Unless and until the FBI can determine they are neither, FBI agents cannot involve U.S. military personnel, because of the bifurcation noted earlier, i.e., under U.S. law, military personnel cannot participate in law enforcement.[88]

The FBI could presumably alert the military to the occurrence of the attacks and let the military conduct its own assessment of the nature of the attacks and need for and propriety of the military's responding to them. To avoid the need to consider whether such action would violate any aspect of U.S. law, we will assume the military is already aware of the attacks and has been conducting its own attempt to ascertain whether they are cybercrime, cyberterrorism or cyberwarfare. We will assume the military has only the information that is available to the FBI, which means its analysis of the nature of the attacks will essentially mirror that of the FBI.

Since the nature of the attacks is inconclusive, the military will need to weigh the risk of responding (perhaps erroneously) against the risk of not responding.[89] Since war

---

law, which means China could legitimately demand that the U.S. turn the agents over to be prosecuted in China. An FBI investigation conducted some years ago prompted such a response. *See, e.g., FSB Hopes to Bring to Court Case against FBI Agents,* Russia & FSU News Bulletin (October 10, 2002), 2002 WLNR 14527663; *Russia: FSB Charges FBI with Hacking,* Infoprod (August 25, 2002), 2002 WLNR 3203882.

[87]*See, e.g., Susan W. Brenner, Cyber Threats, supra* note 8 at 164-176.

[88]*See id.* at 17-18, 177-178.

[89]The FBI faces a similar decision, but the risk of responding erroneously is not as significant in the law enforcement context as it is for the military. *See supra* note 86. If FBI agents responded to the attacks by blocking signals or attacking the computers from which they originated, that *could* be construed as an act of cyberwar. *See id.* The fact that agents of the U.S. government launched the attacks would militate in favor of finding that they constitute cyberwar, since war consists of attacks launched by agents of a sovereign entity. But while agents of the U.S. government launched the attacks, the agents were not members of the U.S. armed forces and, as we saw earlier, only the military "commits" war.

threatens a nation-state's existence, the military may decide the risk of responding outweighs the risk of doing nothing. If it responds, the response will constitute an act of cyberwarfare, the legality of which depends on whether it is offensive or defensive cyberwarfare.[90]

The military will argue that the response constitutes defensive cyberwarfare because they were responding to acts of cyberwar initiated by the Chinese government. Depending on the circumstances, the Chinese government may argue (perhaps quite accurately) that it was not responsible for the attacks that resulted in the U.S. military's attacking computer systems in China. If China truly was not responsible for the attacks, the U.S. military's response will constitute offensive cyberwarfare; and since offensive warfare is unlawful under the laws of warfare, it has committed an illegal act.[91]

These may not be the only scenarios the facts outlined above can support. But I assume they suffice to illustrate my point: A nation-state's ability to respect effectively to a threat ultimately depends on its ability to reliably and expeditiously ascertain what type of threat is at issue. As the sections above demonstrate, when our activities migrate into cyberspace, it becomes correspondingly difficult for nation-states to ascertain the nature of the threats they confront. And as the examples above illustrate, if nation-states cannot reliably ascertain the nature of threats, their ability to respond is impaired, which reduces the disincentives to engage in threat activity.[92] That, in turn, erodes a nation-state's ability to deter and thereby control cyber-threats.

That raises another issue: Since only the military can legitimately wage war, the FBI agents might find themselves being defined as unlawful combatants under the laws of war, which has adverse consequences. *See, e.g.,* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1022-1023.

If China realized the attacks were coming from law enforcement, rather than the military, that should negate the conclusion that they constituted warfare. If the FBI agents realized their counterattacks could be construed as cyberwar, they could ask the Chinese to do something to resolve them and, if Chinese officials did not, alert China that they would be using self-help in an attempt to resolve the situation. That would presumably negate the inference that they constituted cyberwarfare, but it would simply underscore the fact that the FBI agents were about to embark on activity that constituted a crime under Chinese law. *See supra* note 86.

[90]*See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1030-1031 (Article 2(4) of the United Nations Charter "outlaws aggressive war").

[91]*See id.* If the U.S. military's attacking the Chinese computers was not deemed to be an act of war, it could be construed as a crime under Chinese law. *See* Criminal Law of the People's Republic of China – Article 286, Council of Europe Project on Cybercrime, Cybercrime Legislation – People's Republic of China 10 (March 28, 2008), http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20China%20PR%20_28%20Mar%2008_.pdf.

[92]It can also reduce the effectiveness of responses by delaying them until some or all of the intended harm has been inflicted.

It is highly unlikely that the threat identification and response issues outlined above are a transient phenomenon. It is more likely that they will increase in incidence and complexity as our use of computer technology becomes more complex and more pervasive. If that speculation is accurate, we have two choices: We can continue to rely on our current threat identification and response processes for real-world threats and consign cyberspace to the status of outlaw territory, i.e., a "place" in which no state attempts to maintain order. That option is appealing if one assumes, as I do not, that it is possible to segregate cyberspace from real-space; as we saw above, activity in cyberspace has consequences for the physical world. Abandoning cyberspace to lawlessness would only increase the threat activity originating in that domain.

The other choice is to modify our threat identification and response processes in a fashion that improves their ability to response effectively to cyber-threats. Section III examines some efforts that currently seek to do precisely this.

III. Improved Threat Control: Current Efforts

[O]ur cyber-defenses are woefully lacking.[93]

The discussion in § II implicitly assumed that cyberspace is the only factor that is eroding the efficacy of the bifurcated threat-response systems nation-states rely upon to control threats to their existence. That may be true for some countries, but not for the United States. As noted earlier, its arsenal of threat-control structures is larger and more complex than that of other countries.[94] Over the last century, the escalating size and complexity of the U.S. threat-control bureaucracies has increasingly come to impede the efficacy with which the country responds to threats of various types.[95]

In its final report, the 9/11 Commission explained how the balkanized federal bureaucracies severally charged with responding to terrorism and other national security threats unintentionally impeded that process by independently pursuing their respective,

---

The scenario analyzed above simplifies the issues that arise with regard to U.S. response to cyber-threats in at least one respect: It assumes the only players are the U.S. military and the FBI. In reality, such an event would be likely to also involve state and/or local law enforcement officers and, perhaps, agents from other federal agencies, as well as FBI agents. The involvement of officers from additional state, local and/or federal agencies would further exacerbate the command and control and response issues involved in dealing with an attack of the type hypothesized above.

[93]Mike McConnell, *Mike McConnell on How to Win the Cyber-war We're Losing,* Washington Post (February 28, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

[94]*See supra* note 4 and accompanying text.

[95]*See supra* notes 4 & 5 and accompanying text. For the emergence and early growth of bureaucracy in this country, *see, e.g.,* James Q. Wilson, *The Rise of the Bureaucratic State,* 41 Pub. Interest 77, 77-79, 81-91 (1975).

often overlapping agendas.[96] In summarizing the problems, the authors of the report noted that they "learned of the pervasive problems of managing and sharing information across a large and unwieldy government that had been built in a different era to confront different dangers."[97] They also explained that the threat landscape had evolved in the years since these institutions were created, so the country now "confronts . . . challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses."[98] In making that observation, the authors of the 9/11 Commission report were, of course, referring to real-space terrorism.

Members of Congress and other officials have since come to realize that the need for "quick, imaginative, and agile responses" is not limited to the real-space terrorism context. The sections below therefore examine three efforts to meet this need in the context of cyber-threats.

A. Cyber Commands

This section examines how the U.S. military is attempting to improve its efficacy in dealing with the cyber-threats that currently fall within its area of responsibility.[99] As is explained below, this effort involves a series of "Cyber Commands."

1. Creation

On June 23, 2009, the Secretary of Defense directed "the Commander of U.S. Strategic Command"[100] to establish U.S. Cyber Command, ["Cyber Command"] which achieved "Initial Operational Capability" on May 21, 2010.[101] This particular Cyber Command is "a sub-unified command" that is "subordinate to" U.S. Strategic Command and that is composed of the Air Force's Cyber Command, the Army's Cyber Command, the Navy's Fleet Cyber Command, the Marine Corps' Cyberspace Command and the Coast Guard's Cyber Command.[102]

---

[96]Thomas H. Kean & Lee H. Hamilton, 9/11 Commission Report, *supra* note 5 at 399-403. *See also id.* at 73-102.

[97]*Id.* at xvi.

[98]*Id.* at 399.

[99]As § II explained, the military is responsible for protecting the nation from external attacks launched by hostile nation-states.

[100]The U.S. Strategic Command is "a unified command" that is designed to "adapt to the changing international and political landscape". United States Strategic Command, FAQ, http://www.stratcom.mil/faq/.

[101]*See* U.S. Cyber Command, United States Strategic Command, http://www.stratcom.mil/factsheets/cyber_command/.

[102]*See id.* Interestingly, the Cyber Command "fact sheet" only lists the first four entities (Air Force, Army, Navy and Marines) as Cyber Command sub-units. *But see* U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace 5 (July 2011) (Coast Guard Cyber Command is part of U.S. Cyber Command) Lars

To appreciate why Cyber Command was (apparently) established, it is necessary to understand how its subsidiary commands came into existence. The process began in 2005, when the Air Force amended its Mission Statement to state that it will "fight and win" in cyberspace, as well as in air and space.[103] In 2006, the Secretary of the Air Force announced the development of the Air Force Cyber Command, which was to become operational in 2007, but the date was pushed back to October of 2008.[104] At the time, it seemed the Air Force was staking out responsibility for cyberspace, just as it had earlier done for "air" and "space."[105] Then the Air Force put the project on hold to "`make a fresh assessment'" of the proper approach to establishing a cyber command.[106] On August 19, 2009, Air Force Cyber Command became part of the Air Force Space Command.[107]

The Marine Corps' Cyberspace Command was established on January 21, 2010 to protect and defend "the nation's cyberinfrastructure." [108] It "join[ed] a growing list of [Department of Defense] agencies now tasked to support the government's Cyber Command effort." [109] A little over a week later -- on January 29, 2010 -- the Navy's Tenth Fleet, which had been an anti-submarine unit during World War II, was reactivated as the Fleet Cyber Command.[110] It "provides operational support to Navy commanders

---

McCarter, *A Mission Need: Coast Guard Cyber Command,* CGBlog (February 15, 2011), http://cgblog.org/2011/02/15/a-mission-need-coast-guard-cyber-command/ (same). I will assume the Coast Guard Cyber Command is, indeed, a Cyber Command component.

[103]*See, e.g.,* Mitch Gettle, *Air Force Releases New Mission Statement,* U.S. Air Force (December 8, 2005), http://www.af.mil/news/story.asp?storyID=123013440. The prior version stated that the Air Force fought in air and space (only). *See id.*

[104]*See* "Air Force Cyber Command (Provisional)," Wikipedia, http://en.wikipedia.org/wiki/Air_Force_Cyber_Command_(Provisional).

[105]*See, e.g.,* C. Todd Lopez, *Cyber Summit begins at Pentagon Nov. 16,* U.S. Federal News (November 15, 2006), 2006 WLNR 19888715 ("Cyberspace became an official Air Force domain, like air and space, on Dec. 7, 2005" when the new Mission Statement was introduced). *See also* C. Todd Lopez, *Air Force Leaders to Discuss New "Cyber Command,"* U.S. Federal News (October 5, 2006), 2006 WLNR 17319253.

[106]*See* "Air Force Cyber Command (Provisional)," *supra* note 104 (quoting *On Pause, But Not Abandoning,* Air Force Magazine (August 14, 2008).

[107]*See* "Air Force Cyber Command (Provisional)," Wikipedia, *supra.*

[108]*See* Alan J. McCombs, *Marines Launch into Cyberspace with New Command,* Fort Meade (January 28, 2010), http://www.ftmeade.army.mil/pages/news/stories/2010/jan/cyber.html.

[109]*Id.*

[110]See "United States Tenth Fleet," Wikipedia, http://en.wikipedia.org/wiki/United_States_Tenth_Fleet.

worldwide" for "information, computer [and] electronic warfare".[111] The Coast Guard's Cyber Command was created in May or June of 2010.[112] Its mission is to protect Coast Guard computer systems and data, "[l]everage cyberspace as a force multiplier" for Coast Guard missions and protect the marine transportation system and critical infrastructure from cyber attacks.[113] And, finally, on October 1, 2010 the Army established its Cyber Command "to plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all Army networks."[114]

To an observer, it might seem peculiar that all five branches of the U.S. military found it necessary to establish a unit-specific cyber command, and do so in a relatively truncated time frame. The explanation for this phenomenon lies in two, unrelated factors, one of which is that the threat of cyberwar received a great deal of media attention in the year or so prior to the Air Force's revising its mission statement.[115] The publicity raised awareness of the need for a cyberwar response effort, and "Air Force leaders" decided their branch should be "the lead service in cyber warfare" (for reasons I speculate about in a moment).[116] This, plus the creation of the Air Force Cyber Command, triggered a turf war among the various branches, which resulted in the creation of five idiosyncratic yet substantially overlapping cyber commands.[117]

---

[111]*See, e.g.,* Joseph E. Sisson, *Fleet Cyber Command/ TENTH Fleet: Enabling Cyber Unity of Effort* 14*,* Naval War College (May 3, 2010), http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA525307.

[112]*See, e.g.,* Amber Corrin, *Cyber Command Lays Groundwork for Rapid Deployment of Resources,* Government Computer News (June 9, 2010), http://gcn.com/articles/2010/07/09/cyber-command-panel-afcea-symposium.aspx; Geoff Fein, *Cyber Commands Gain Traction, Services Vulnerable To Power Grid Attacks*, Defense Daily (May 6, 2010), 2010 WLNR 10703214.

[113]*See* Lars McCarter, *A Mission Need: Coast Guard Cyber Command, supra* note 102.

[114] "U.S. Army Cyber Command," Wikipedia, http://en.wikipedia.org/wiki/U.S._Army_Cyber_Command.

[115]*See, e.g., CIA Official Says Cybersecurity Threats Evolving Faster than Defense,* Inside the Pentagon (July 29, 2004), 2004 WLNR 82077. *See also U.S. Government Well Defended against Cyber-Attacks, State Says,* U.S. Federal News (August 26, 2005), 2005 WLNR 13609747; *Communicators Train to Face Enemies on Digital Battlefield,* Regulatory Intelligence Data (December 13, 2004)

[116]*See, e.g., New Mission Statement Isn't Really for Airman,* Air Force Times (December 26, 2005), 2005 WLNR 27580984.

[117]*See id.* (Air Force's desire to be the dominant service in cyberspace was "about turf", specifically about its rivalry with the Navy); Shane Harris, *The Cyberwar Plan,* National Journal (November 13, 2009), 2009 WLNR 23121431 (the four branches "competed with one another to control the military's overall strategy"). *See also* Kevin Coleman, *Inside the Cyber Command Turf Battle,* Defense Tech (August 15, 2008), http://defensetech.org/2008/08/15/inside-the-cyber-command-turf-battle/.

That brings us to the second factor that contributed to this state of affairs: The United States has five military branches, each with a distinct legacy mission, because of history: Armies, like the U.S. Army, evolved to fight land battles;[118] navies, like the U.S. Navy, evolved to fight sea battles;[119] the U.S. Marines evolved as an amphibious fighting force[120]; the U.S. Coast Guard was created to control smuggling and has evolved into a maritime law enforcement agency that can also perform military functions;[121] and the U.S. Air Force evolved to conduct military operations in the air.[122]

This segmentation of responsibility for responding to external threats is a logical strategy in a world in which threats are territorially based.[123] In that world, the response to an external threat (the Japanese attack on Pearl Harbor, say) focuses on a clearly identified, clearly identifiable enemy and, at least for the United States, has for the most part been conducted offshore. In an era dominated by territorially-based threat activity, it was reasonable to divide the response into (i) engaging the enemy on land, (ii) engaging the enemy at sea, (iii) engaging the enemy in and by virtue of exploiting airspace and (iv) ensuring the naval response effort could support the delivery of land forces when and as needed. The Coast Guard's role has historically involved more law enforcement and other non-military activities, but it is officially a branch of the U.S. armed services and operates under the authority of the Navy when the country is at war.[124]

As we saw in § II, threats are no longer necessarily land-based; they transcend national boundaries. The change in this aspect of threats has consequences for the bifurcated threat-control system on which sovereign entities continue to rely. Aside from anything else, it raises two issues, one of which is a subset of the other. The broader issue is whether the bifurcated external-internal[125] threat response approach is still viable in the twenty-first century.

We will not address that issue because an analysis of the overall efficacy of the bifurcated response approach is outside the scope of this article for two reasons, the first of which is that such an analysis cannot focus exclusively on cyber-threats. It must also encompass land-based threats and as noted above, the bifurcated approach remains a

---

[118]*See, e.g.,* "United States Army," Wikipedia, http://en.wikipedia.org/wiki/United_States_Army.

[119]*See, e.g.,* "United States Navy," Wikipedia, http://en.wikipedia.org/wiki/United_States_Navy.

[120]*See, e.g.,* Mission, TheUSMarines.com, http://www.theusmarines.com/mission/.

[121]*See* Missions, U.S. Coast Guard, http://www.uscg.mil/top/missions/.

[122]*See* History, U.S. Air Force, http://www.airforce.com/learn-about/history/.

[123]*See supra* § II.

[124]*See* 14 U.S. Code § 1. *See also* Missions, U.S. Coast Guard, *supra* note 121.

[125]I shall continue to use these terms to differentiate crime/terrorism and war even though they are not entirely accurate as threats migrate into cyberspace. *See supra* § II.

satisfactory way to control these threats, which will persist.[126] It would therefore be imprudent to decide nation-states should jettison a strategy that is still effective against what will no doubt continue to be, if not the most common, the most serious threats they confront because it is not a satisfactory way to control cyber-threats.[127]Conversely, it would be equally imprudent to conclude that because the bifurcated approach is an effective way to deal with land-based threats, we should continue to employ it for *all* threats, despite its relative inefficacy against cyber-threats. There is, however, is a third option: Conclude that the bifurcated approach (i) is effective against land-based threats but (ii) is not, at least as it is currently configured, effective against cyber-threats and (iii) develop a new approach for dealing with cyber-threats.

That brings me to the other reason why we are not pursuing the broader issue noted above. My purpose in writing this article is to analyze the extent to which the way we currently structure the bifurcated approach actually impedes our ability to address cyber-threats and to speculate about whether we can modify that structure and thereby improve this approach's efficacy against cyber-threats. This undertaking differs from the first two options noted above, both of which focus on the overall viability of a bifurcated approach and therefore require a zero-sum resolution: We would either (i) decide that the bifurcated approach is our only option and therefore retain it for both land-based and cyber-threats or (ii) decide that because it is not effective (enough) against cyber-threats we must resort to an alternative, presumably a unitary approach in which a single institution is responsible for controlling *all* threats.

As I noted in § II(D), the first option is unacceptable because it would consign cyberspace to a state of lawlessness. As to the second option, I, for one, do not see the need for such drastic action.[128] I think the preferable course is to concede that the bifurcated approach, as it is currently configured, is not an effective against cyber-threats and then analyze how it can be reconfigured to improve its efficacy in this regard.

I see this as the most pressing, and more manageable, of the two issues. The remainder of this section undertakes the first task noted above: It reviews how the United States structures the bifurcated approach and analyzes the extent to which this impedes the country's response to cyber-threats. Section III(A)(2) examines the military; section III(B) examines law enforcement; and § III(C) reviews proposed legislation that is designed to incorporate civilian participation into the efforts of either or both. Section IV

---

[126]As to why they will persist, *see, e.g.,* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* at 20-46. It is reasonable to assume, at least for the present, that certain crimes, such as rape, assault and theft of tangible items, will necessarily be confined to the physical world. It is also reasonable to assume that intra-sovereign conflicts will continue to emphasize kinetic force, as well as cyber-force, at least to the extent that one sovereign seeks to expand its control over physical territory and assets.

[127]As to why the approach is not effective in controlling cyber-threats, *see supra* § II.

[128]Relying on a unitary entity to conduct both law enforcement and military functions would violate federal law, and perhaps the Constitution. *See, e.g., Susan W. Brenner, Cyber Threats, supra* note 8 at 164-176.

then speculates about how we might modify this structure and thereby improve the bifurcated approach's efficacy against cyber-threats.

2. Analysis

As we saw above, the U.S. military now has six cyber commands: one for each of the respective branches of the military plus the overarching Cyber Command.[129] As we also saw above, each of the five branches (i) was created to carry out a distinctive component of land-based warfare and (ii) has adopted a mission statement for its cyber command that summarizes what that command is intended to accomplish:

- The Air Force's cyber command fights and wins in cyberspace.
- The Marine Corp's cyber command defends the nation's cyberinfrastructure.
- The Navy's cyber command provides operational support to Navy commanders engaged in cyberwarfare.
- The Coast Guard's cyber command protects the marine transportation system and critical infrastructure from cyberwarfare.
- The Army's cyber command plans, coordinates and conducts cyberwarfare.

As I noted in § III(A)(1), the legacy missions of the branches overlap, at least to some extent, when the United States is at war because they work together to defeat the enemy. Their contributions are not, of course indistinguishable. In wartime, four of the branches (Air Force, Army, Marine Corps and Navy) each has a specific, complementary role to play, and the Coast Guard becomes part of the Navy.[130]

Logically, then, it is reasonable to assume that the respective cyber commands will play a correlate role in cyberwarfare, i.e., each will have a distinctive contribution to make to such an effort. But if we parse their respective missions, that does not appear to be the case. Three of the mission statements – the Air Force's, the Navy's and the Army's – simply state that the branch's cyber command will participate in cyberwarfare; they in no way differentiate the contribution(s) each will make to that effort. The Marine Corps' and Coast Guard's mission statements can be interpreted the same way.[131]

---

[129]From this point forward, I will use "cyber command" to denote one of the branch cyber-units and Cyber Command to denote the overarching entity.

[130]*See supra* § III(A)(1).

[131]One *could* argue that by pledging to defend/protect the country's critical infrastructure the Marine Corps and the Coast Guard might be pledging to utilize kinetic force, as well as cyber-force, in this regard. The other mission statements seem to contemplate only non-kinetic activity. For the present, there is, at least, a tacit assumption that cyber-force will be met only with cyber-force, to avoid the risks of escalating a digital conflict into something more devastating. *See, e.g., Cyber Warfare: Rising Risks and Implications,* Emerging Markets Online (September 13, 2010), 2010 WLNR 18254196. *See also* Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny,* 12 N.C. J. L. & Tech. On. 1, 18-24 (2010).

This inferentially suggests that there is no doctrinal or operational differentiation among the roles the respective commands would play in cyberspace.[132] The validity of that inference is further supported by the fact that "cyberspace" denotes an experiential, rather than spatial, phenomenon.[133] There is therefore no way to parse the respective branches' contributions to a cyberwarfare effort according to the various "dimensions" of cyberspace.

The Department of Defense created Cyber Command because it recognized this.[134] According to a knowledgeable source, the new command was created to take "operational control of disparate cyber-security and attack units that had been scattered among the four military services.[135]

Cyber Command has so far made little progress toward achieving this goal.[136] In 2011, the Government Accountability Office issued a report in that was strongly critical of

---

[132]*See, e.g., Disjointed, Redundant Cybersecurity Programs Undermine Efforts to Protect Networks,* National Defense (July 18, 2011), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=470. *See also* U.S. Government Accountability Office, Defense Department Cyber Efforts 17 (May 2011), http://www.gao.gov/products/GAO-11-421 (branches "are pursuing diverse service-specific approaches to establishing cyberspace capabilities because . . . U.S. Cyber Command has . . . not fully defined long-term mission requirements and capabilities for [them] to fulfill").

[133]*See, e.g.,* Joseph Schmitt & Peter Nikolai, *Application of Personal Jurisdiction Principles of Electronic Commerce: A User's Guide,* 27 Wm. Mitchell L. Rev. 1571, 1577-1578 (2001) (William Gibson used "cyberspace" to refer to "the non-existent space where computer communication takes place"). *See also* William Gibson, Neuromancer 51 (1984) (describing cyberspace as a "consensual hallucination that felt and looked like physical space but actually was a computer-generated construct").

[134]*See* U.S. Cyber Command, *supra* note 101 (new command "will centralize command of cyberspace operations").

[135]Seymour Hersh, *The Online Threat,* The New Yorker (November 1, 2010), http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh?currentPage=all. Cyber Command's designated tasks are to lead

> day-to-day defense and protection of [Department of Defense] information networks; coordinate operations providing support to military missions; direct the operations and defense of specified [Department of Defense] information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations.

U.S. Cyber Command, *supra* note 101.

[136]*See, e.g.,* U.S. Government Accountability Office, Defense Department Cyber Efforts 17 (May 2011), http://www.gao.gov/products/GAO-11-421 (commands "are pursuing diverse service-specific approaches to establishing cyberspace capabilities because . . . Cyber Command has . . . not fully defined long-term mission requirements and

Cyber Command; among other things, the report said it needs to specify "the structure and duties of the Army, Navy, Air Force and Marine cyber components."[137] A spokesman for Cyber Command said it was addressing these issues, but "there is currently no `timeline for completion.'"[138]

Before Cyber Command was created, some members of the military argued that branch-specific commands could not provide an effective cyberwar response system.[139] They claimed the "cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare."[140]And they contended that the "core skills" needed to wage cyberwar differ radically from those needed for conventional war.[141] Those who subscribed to this view believed the better approach was to create a new, cyber-specific branch of the military and assign it overall responsibility for cyber operations, just as the Air Force was assigned responsibility for air operations.[142]

I suspect that view did not prevail because it would have required the various branches to give up their cyber commands. Since it has for some time been apparent that cyberspace can be used for military purposes, I suspect the five branches were reluctant to give up the opportunity to play a role in this new theatre of combat. I also suspect that the proposal to create a new, cyber-specific branch of the U.S. military may

---

capabilities"). *See also* Army Cyber Command, 2011 Army Posture Statement, https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/information_papers/PostedDocument.asp?id=256 (Army cyber command has incorporated "existing cyber forces" into a new unit, U.S. Army Cyber Command/2d Army, and in 2011 "will stand up a Cyber Brigade" to expand its capability in cyberspace).

[137]Lolita C. Baldor, *Report Says Pentagon Should Boost Cyber Staff,* Air Force Times (June 20, 2011), http://www.airforcetimes.com/news/2011/06/ap-military-pentagon-should-boost-cyber-staff-report-says-062011/. As one observer noted, "fissures between the services and even within the cyber command make it hard to come up with timetables to update policies, response plans and technology roadmaps." Kevin Fogerty, *Is It Time for the Pentagon to Turn Cyberwar Over to Someone Else?,* IT World (July 29, 2011), http://www.itworld.com/node/187699?source=cotd. *See also id.* ("The overall picture the GAO paints is of fragmented military organization with no clear direction or goal to pursue in cybersecurity").

[138]Tiffany Kaiser, *GAO Report: Pentagon Must Provide Better Training for New Cyber Command Security System,* Daily Tech (June 21, 2011), http://www.dailytech.com/GAO+Report+Pentagon+Must+Provide+Better+Training+for+New+Cyber+Command+Security+System/article21963.htm.

[139]*See, e.g.,* Gregory Conti & John "Buck" Surdu, *Army, Navy, Air Force and Cyber – Is It time for a Cyberwarfare Branch of the Military?,* IAnewsletter (Spring 2009) http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf.

[140]*Id.* at 16.

[141]*See id.*

[142]*See id.* at 17.

not have prevailed because it would have been difficult, if not impossible, to implement. As we saw above, the rationale for the different branches is that each is responsible for military activity in a specific spatial domain in the physical world.[143] While the divisions are not precise, it is far easier to parse response authority in a spatial context than it is with regard to cyberspace.

Cyberspace operations do not take place in a physical place; instead, they involve activity that occurs in and through computer technology, which is pervasive in today's world. If the Department of Defense had chosen to create a distinct branch with exclusive combat authority in cyberspace, it would presumably mean this branch would take command of any and all of the other branches' activities that involved cyberspace. It is difficult to see how this could be a viable strategy. It would presumably mean, for example, that members of the cyber-branch would monitor, and probably control, the other branches' computers and online activities (i) to ensure a baseline of security and (ii) to be in a position to respond if and when the cyber-branch believed it necessary to deter or respond to cyberwarfare attacks. That seems to be the only way to functionally allocate operational responsibility in cyberspace to a new, cyber-specific branch of the U.S. military.

If that is, indeed, the only way to accomplish this, then instead of participating in a carefully defined, complementary division of responsibility such as the one the existing branches currently represent, the hypothesized cyber-branch would essentially subsume the other branches as to its distinct area of responsibility. And that could be problematic. It might, for example, create clashes of authority that could have negative consequences for the U.S.' ability to respond to cyber attacks.[144]

This might be one of the reasons the Defense Department apparently opted, instead, to create a distinct command that unified the cyberspace components of the five traditional branches of the military. This approach is fraught with its own problems, the most obvious of which is coordinating the activities of the five branch cyber commands. If cyberspace were divisible into spatial operational domains, Cyber Command could function in a fashion analogous to that of one of the U.S. military's conventional Unified Combatant Commands.[145]These Commands incorporate personnel from the five military

---

[143]*See supra* § III(A)(1).

[144]Assume, say, that a hostile state's own cyberwarriors use "cyberattacks to alter data, such as logistics plans" stored in U.S. military computers. Duncan B. Hollis, *An E-SOS for Cyberspace,* 52 Harv. J. Int'l L. 373, 388 (2011). Assume the plans at issue were created by and are to be used by the U.S. Army; also assume that the hypothesized U.S. Cyber Branch is in charge of the Army's computers when the attack strikes them. Would Army personnel be content to stand by idly as the Cyber Branch personnel dealt with the attack? Or would they want to participate in or take charge of responding to the attack? Might the two have different priorities? The Army might see preserving the integrity (and confidentiality) of the plans as the primary objective, which would presumably involve only defensive measures. The Cyber Branch's main concern, on the other hand, might well be responding to the attack, which could involve launching offensive attacks against the attacking cyberwarriors.

[145]*See, e.g.,* U.S. Department of Defense, Unified Command Plan, http://www.defense.gov/home/features/2009/0109_unifiedcommand/.

branches into a unified command with responsibility for a specific geographical area.[146] The personnel assigned to such a Command respectively carry out the functions that are within their branch's unique expertise, e.g., the Navy carries out operations at sea, the Air Force conducts aerial activities and so forth.

As we saw above, cyberspace, unlike real-space, cannot be parsed into spatial domains. Unless and until that changes, Cyber Command faces the unenviable task of trying to sort out what, precisely, should be the respective responsibility of the Air Force, Army, Marine and Navy cyber commands. At the moment, it appears that at least these four cyber commands have essentially the same mission, i.e., to conduct offensive and defensive military operations in cyberspace.[147]This is not only pointless, it is likely to be counterproductive. Unfortunately, as we also saw above, this state of affairs seems likely to continue for some time.[148]

And there is yet another issue Cyber Command must resolve. Since the task list cited earlier[149] focuses exclusively on (i) defending the military's assets in cyberspace and (ii) directing and conducting military operations in cyberspace, many wondered if the new Cyber Command was *only* going to be responsible for protecting military assets and networks. In other words, is Cyber Command also responsible for protecting civilians and civilian-owned assets?

In the fall of 2010, the newly-appointed head of Cyber Command, General Keith Alexander told reporters the new unit did "not have a role" in protecting civilian networks and cyber-assets.[150] This caused controversy because, as § II noted, the military's role has historically been to protect a state, its citizens and their assets from external threats. If General Alexander's comment were transposed to the context of kinetic warfare, it would become a declaration that in the event of nuclear war the U.S. military will protect itself but not civilians. Since that proposition is completely inconsistent with the military's role in society, it is not surprising that the general at least to some extent retreated from that position in a statement he made the next day.

---

[146]*See, e.g.,* Fact Sheet: United States Africa Command, http://www.africom.mil/getArticle.asp?art=1644.

[147]*See supra* § III(A)(1). *See also supra* note 136. The Department of Defense's Strategy for Operating in Cyberspace, which it released in July of 2011, does not address how the roles of these branches, at least, could be structured to make them complementary. *See* Strategy for Operating in Cyberspace, *supra* note 102.

[148]*See supra* notes 136 - 138 & accompanying text. *See also* Kathleen Hickey, DOD's Cyber Strategy Lacks Organization, Manpower and Funds, GAO Says, Government Computer Network (July 26, 2011), http://gcn.com/articles/2011/07/26/dod-cyber-strategy-weaknesses-gao.aspx.

[149]*See supra* note 135 & accompanying text.

[150]Noah Shachtman, *Military's Cyber Commander Swears: "No Role" in Civilian Networks,* Wired (September 23, 2010), http://www.wired.com/dangerroom/tag/cybersecurity/page/2/.

In testifying before the House Armed Services Committee, General Alexander said Cyber Command "could have a broader role in the civilian infrastructure through protecting US critical infrastructure networks and systems."[151]He noted, though, that the White House "was examining the legal authority needed" for Cyber Command to take responsibility for protecting civilians and civilian-owned assets.[152] A few days later, the Department of Defense and the Department of Homeland Security[153] perhaps sought to address this issue, at least in part, by signing a memorandum of understanding that (i) gives Homeland Security "lead responsibility for protecting the U.S. government's civilian networks and critical infrastructure", (ii) makes the Defense Department responsible for "protecting some 15,000 military networks" and (iii) provides that the two will collaborate to "safeguard cyberspace against state as well as nonstate actors."[154]

Both General Alexander's comments and the memorandum of understanding executed by the Departments of Defense and Homeland Security demonstrate the doctrinal and institutional constraints that impede the United States' ability to mount a unified response to cyber-threats. The primary constraint is the bifurcation described in § II: The military (Defense) deals with war, while law enforcement (Homeland

---

[151]*White House Seeks Expansion of Cyber Command's Civilian Cybersecurity Authority,* Infosecurity (September 24, 2010), http://www.infosecurity-us.com/view/12744/white-house-seeks-expansion-of-cyber-commands-civilian-cybersecurity-authority/.

[152]*See id.* As noted earlier, under U.S. law the military is barred from participating in law enforcement efforts. *See supra* note 84 & accompanying text.

[153]The Department of Homeland Security is charged with protecting citizens of the United States from internal threats, especially terrorism. *See, e.g.,* One Team, One Mission, U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013, 2-3, http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf.

[154]Donna Miles, *DOD, Homeland Security Collaborate in Cyber Realm,* Info Wars (June 3, 2011), http://www.infowars.com/dod-homeland-security-collaborate-in-cyber-realm/. *See* Joint Statement by Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano on Enhancing Coordination to Secure America's Cyber Networks (October 13, 2010), http://www.dhs.gov/ynews/releases/pr_1286984200944.shtm; Memorandum of Agreement between the Department of Homeland Security and The Department of Defense Regarding Cybersecurity (September 27, 2010), http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf. *See also* U.S. Department of Defense Strategy for Operating in Cyberspace 8-9 (July 2011), http://www.defense.gov/news/d20110714cyber.pdf . The reference to Homeland Security's responsibility for protecting *government* civilian networks seems to mean just that. *See, e.g.,* Testimony of National Cybersecurity and Communications Integration Center Director Sean McGurk, NPPD, before the House Committee on Oversight and Government Reform, Subcommittee on National Security, Homeland Defense and Foreign Operations (May 25, 2011), http://www.dhs.gov/ynews/testimony/testimony_1306421842051.shtm. *But see id.* (Homeland Security also "works with" private sector "owners and operators" of critical infrastructure components to "bolster their cybersecurity preparedness").

Security)[155] deals with crime and terrorism. Due to historical circumstance, the bifurcation implicitly assumes attacks from abroad target nation-state assets and/or personnel while crime and terrorism target civilian assets and/or personnel.

As we saw in § II, that is not necessarily true as threats migrate into cyberspace. Civilians and civilian-owned assets are already a target of cybercrime and cyberterrorism, and it has for some time been apparent that they will also be targets in cyberwarfare.[156] The bifurcation, though, does not allow (i) law enforcement officers to retaliate against cyberwarfare attacks or (ii) members of the military to retaliate against cybercrime and cyberterrorism. That is why General Alexander could not assert that Cyber Command would protect civilians, and that is why the Departments of Defense and Homeland Security found it necessary to execute the memorandum of understanding noted above.

As matters currently stand, Cyber Command will have to utilize the attribution processes described in § II to determine, with the necessary level of confidence, that a given attack was state-sponsored before it can reciprocate in kind. Civilians and civilian assets have been targets of conventional warfare, even though the law of armed conflict calls for minimizing attacks on noncombatants.[157] But those attacks have come from an identified, nation-state enemy, which allowed the targeted nation-state to respond in kind, even if the attack occurred on its territory.[158]

General Alexander's primary problem, therefore, is that it may be impossible for the military to make such a determination for a cyberattack quickly enough for a timely response because the "markers" traditionally used to distinguish between internal and external attacks are of little utility in the cyber context. This is essentially a doctrinal problem, as it arises from the practice of dividing threats into these two categories and

---

[155]I put the Department of Homeland Security in the law enforcement category for several reasons: One is that it is a civilian, rather than military, agency; another is that many of its responsibilities involve law enforcement or quasi-law enforcement functions. *See, e.g.,* Department of Homeland Security Mission and Responsibilities, Department of Homeland Security, http://www.dhs.gov/xabout/responsibilities.shtm. A third reason is that the Department incorporates agencies that perform law enforcement functions. *See* Appendix D: DHS Organizational Chart, U.S. Department of Homeland Security Strategic Plan Fiscal Years 2008-2013, *supra* note 153.

[156]*See, e.g.,* Eric Talbot Jensen, *Cyber Warfare and Precautions against the Effects of Attacks,* 88 Tex. L. Rev. 1533, 1551-1552 (2010); Charles J. Dunlap, Jr., *Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors,* 87 Neb. L. Rev. 712, 723 n. 40 (2009).

[157]*See* Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts art. 51(3), adopted on June 8, 1977, 1125 U.N.T.S. 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13(3), adopted on June 8, 1977, 1125 U.N.T.S. 609.

[158]*See, e.g.,* "The Blitz," Wikipedia, http://en.wikipedia.org/wiki/The_Blitz.

categorically parsing threat response authority between them.[159] But as we saw earlier, General Alexander also confronts an institutional problem: fusing six distinct cyber commands into a coordinated, coherent cyber-response effort.[160] We will return to this issue in § IV, *infra.*

As we will see below, U.S. law enforcement confronts a correlate doctrinal problem and operates in a far more complex institutional structure.

B. Law Enforcement

As we saw in § II, law enforcement is charged with controlling the "other" threat: the threat to internal order that arises from antisocial conduct on the part of individuals who are "in" the territory of the state under whose authority law enforcement officers operate.[161] Some countries have a national penal code and a national police agency that enforces that code.[162] But because it is a federal state,[163] the United States has an essentially two-tiered system of penal laws and a two-tiered law enforcement structure.

As to the former, the United States has fifty-two distinct criminal codes (one for each state, one for the District of Columbia and a federal criminal code).[164] These codes

---

[159]It also arises from the fact that our definitions of war assume traditional, kinetic conflict. *See, e.g.,* Article 51, United Nations Charter, http://www.un.org/en/documents/charter/chapter7.shtml ("armed attack"); Article I, Definition of Aggression, United Nations General Assembly Resolution 3314 (XXIX), http://www1.umn.edu/humanrts/instree/GAres3314.html ("use of armed force"). The United States has made little, if any, progress toward reconciling the law of war and cyber attacks. *See, e.g.,* David Lerman, *Senators Demand Answers on U.S. Cyber Warfare Policy,* Bloomberg (July 20, 2011), http://www.bloomberg.com/news/2011-07-20/senators-demand-answers-on-u-s-cyber-warfare-policy.html.

[160]*See, e.g., supra* note 137.

[161]As § II explained, nation-states control such conduct by adopting laws that outlaw such behavior and impose sanctions on those who engage in it.

[162]*See, e.g.,* Kuk Cho, *Korean Criminal Law: Moralist Prima Ratio for Social Control,* 1 J. Korean Law 71, 73-84 (2001), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=289401; "National Police Agency (Republic of Korea)," Wikipedia, http://en.wikipedia.org/wiki/National_Police_Agency_(South_Korea).

[163]*See, e.g.,* Steven G. Calabresi & Nicholas Terrell, *The Number of States and the Economics of American Federalism*, 63 Fla. L. Rev. 1, 2 (2011) (with fifty states the United States is the largest federation in the world).

[164]*See, e.g.,* Paul H. Robinson & Marcus D. Dubber, *The American Model Penal Code: A Brief Overview,* 10 New Crim. L. Rev. 319, 319 (2007) ("Within the United States, there are fifty-two . . . criminal codes, with the federal criminal code overlaying the codes of each of the fifty states and the District of Columbia").

require a corresponding, two-tiered law enforcement structure: One tier consists of the over 15,000 state and local agencies[165] that respectively enforce state criminal codes.[166] Their geographical jurisdiction is generally linked to the nature of the agency in which they serve: State police have jurisdiction throughout the state, a county sheriff has jurisdiction in that county and municipal police have jurisdiction within the territorial boundaries of their municipality.[167]

The other tier is composed of agencies that enforce federal law. Five of them – the Federal Bureau of Investigation, the U.S. Secret Service, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Drug Enforcement Administration and U.S. Immigration and Customs Enforcement -- are primarily responsible for pursing those who violate the federal criminal code.[168] And because these agencies operate under the

---

Title 18 of the U.S. Code is often referred to as the "federal criminal code" because it contains the vast majority of federal criminal provisions. *See, e.g.,* "Title 18 of the U.S. Code," Wikipedia, http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code; Jude Pamela Mathy, *Honest Services Fraud after Skilling,* 42 St. Mary's L.J. 645, 702 n. 273 (2011) ("The Federal Criminal Code codified in title 18"). Other titles of the U.S. Code, however, create additional crimes. *See, e.g.,* Bruce Zagaris, *U.S. International Cooperation against Transnational Organized Crime,* 44 Wayne L. Rev. 1401, 1427 (1993) (noting the "drug crimes in Title 21 . . . of the United States Code"); U.S. Department of Justice Tax Division, Criminal Tax Manual, Table of Contents (2008), http://www.justice.gov/tax/readingroom/2008ctm/CTM%20TOC.htm (Title 26 of the U.S. Code creates federal tax crimes).

[165]*See supra* note 4. State agencies, which are variously known as State Police, Highway Patrol or State Patrol, operate statewide. *See, e.g.,* "Law Enforcement in the United States," Wikipedia, http://en.wikipedia.org/wiki/U.S._law_enforcement. Local law enforcement consists of county agencies, e.g., Sheriff's or County Police agencies, and municipal law enforcement agencies. *See id.*

[166]For our purposes, "state law" includes both the laws adopted at the state level and any laws adopted by subdivisions of a state. *See, e.g.,* Alaska Stat. § 18.65.080 (state troopers enforce "all criminal laws of the state"); Colo. Rev. Stat. § 16.2.5-103(1) (sheriff's authority includes enforcing all laws of the state); Nev. Rev. Stat. § 493.190 (municipal officers responsible for enforcing "state and municipal laws").

[167]*See* "State Police: United States," Wikipedia, http://en.wikipedia.org/wiki/State_Police#United_States; "Sheriffs in the United States," Wikipedia, http://en.wikipedia.org/wiki/Sheriffs_in_the_United_States; "Law Enforcement in the United States: Municipal," Wikipedia, http://en.wikipedia.org/wiki/Law_enforcement_in_the_United_States#State. *See, e.g.,* 11 Del. Code § 8302 (state police "primary law enforcement agency within the State"); Wash. Rev. Code § 36.28.010 (sheriff is "conservator of the peace of the county"); 42 Pa. Cons. Stat. § 8951 (municipal officer has jurisdiction "within the territorial limits of a municipality").

[168]*See* Susan W. Brenner, Cyber Threats, *supra* note 8 at 152-153. *See, e.g.,* 18 U.S. code § 3052 (Federal Bureau of Investigation); 18 U.S. Code §§ 1029(d), 1030(d)(1) 3056 (Secret Service); 18 U.S. Code § 3051 (Bureau of Alcohol, Tobacco, Firearms and Explosives); 21 U.S. Code § 878 (Drug Enforcement Administration); 19 U.S. Code §

authority of the federal government, they have national jurisdiction, i.e., their agents can pursue investigations anywhere that is within the "maritime and territorial jurisdiction of the United States"[169] and, under certain circumstances, abroad.[170]

It may seem that this complex enforcement structure, with its often-overlapping federal and state jurisdiction, must inevitably generate turf wars that impede the efficient enforcement of the law. The likelihood that rivalry will occur between state and local law enforcement agencies is mitigated, at least to some extent, by the fact that each has a clearly defined geographical jurisdiction within which it operates.[171] This reduces, but does not eliminate, the potential for inter-agency conflicts.[172] Instances can, and do, arise in which, say, the State Police and the County Sheriff both have jurisdiction in a given matter,[173]which can create conflicts as to who should take the lead.[174] Over the last few years, state and local agencies have used multi-jurisdictional task forces to reduce, if not eliminate, such conflicts.[175]

1589a, 22 C.F.R. § 127.4 (Immigration and Customs Enforcement). Immigration and Customs Enforcement is divided into "four law enforcement divisions", each with its own mission. "U.S. Immigration and Customs Enforcement," Wikipedia, http://en.wikipedia.org/wiki/U.S._Immigration_and_Customs_Enforcement. For other agencies that play a less significant role in federal law enforcement, *see, e.g.,* "Law Enforcement in the United States," *supra* note 165.

[169]18 U.S. Code § 7.

[170]Federal courts presume that when Congress enacts a federal criminal statute, it only means for the law to be enforceable within the territorial jurisdiction of the United States. *See, e.g.,* United States v. Corey, 232 F.3d 1166, 1170 (9th Cir. 2000). If Congress indicates that a statute is enforceable outside U.S. territory, courts will apply the law in that manner. *See id. See, e.g.,* 18 U.S. Code § 1030(e)(2)(b) (extraterritorial jurisdiction under the federal computer crime statute).

[171]*See, e.g., supra* note 167.

[172]Funding can be a source of conflict. *See, e.g., Sheriffs: State Police Duplicate Our Efforts,* Detroit News B1 (September 7, 2005), 2005 WLNR 26971791.

[173]A homicide could create an even more complicated scenario: Assume John Doe is found murdered in his home, which is in Garden City, Finney County, Kansas. *See, e.g.,* "Garden City," Wikipedia, http://en.wikipedia.org/wiki/Garden_City,_Kansas. The Garden City police, the Finney County Sheriff and the Kansas Highway Patrol would all have jurisdiction to investigate the crime. *See, e.g., supra* note 166.

[174]*See, e.g., Troopers Absent At City Turf Hearing,* Boston Globe 1 (June 29, 2011); *Carson Beach: Whose Turf Is It?,* Boston Globe 15 (June 2, 2011); Reid J. Epstein, *Suffolk Rejects Funds for Bomb Dog,* Newsday A 15 (December 23, 2010).

[175]*See, e.g.,* Ron Jackson, *Task Force Sought for Pending Cases,* The Oklahoman 7A (December 2, 2009); Robert Medley & Michael Kimball, *3 Oklahoma City Residents Jailed in Kansas after Crime Spree,* The Oklahoman (November 3, 2010). The use of task forces apparently dates back to the 1970s. *See, e.g.,* Anne C. Pogue, *If It Weren't for the Flip Side,* 14 Cornell J. L. & Pub. Pol'y 477, 481 (2005).

Historically, the more serious conflicts arose between state and local agencies and their federal counterparts.[176]There appears to have been a corresponding reduction in these conflicts, as well, a phenomenon many attribute to a spirit of greater cooperation brought on by the 9/11 attacks.[177]

That leaves the federal agencies, which have certainly not been immune to turf wars.[178] And according to recent reports, turf battles continue to be a problem for federal law enforcement agencies, despite their use of task forces and other, similar efforts.[179] One reason why such conflicts persist among federal agencies is that, unlike their state and local counterparts, the federal agencies' jurisdictional authority is predicated not on geographical turf, but on what a recent report refers to as "operational turf."[180]

In situations like the hypothetical noted earlier,[181] in which a crime scene falls within the State Police's and the local Sheriff's geographical turf, the State Police may

---

[176]*See* Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism,* 34 Crime & Just, 377, 405 (2006). *See, e.g.,* David McLemore, *Interdiction Not Answer, Officers Say,* Dallas Morning News (August 30, 1988), 1988 WLNR 2258214 (noting "continuing turf battles among federal and state law enforcement agencies"). *See also* Pierre Thomas, *Freeh Becomes Fifth Director of FBI,* Washington Post A06 (September 2, 1998), 1993 WLNR 5381516 (new director pledge to end "turf battles" among "federal, state and local law enforcement").

[177]*See, e.g.,* Stephen D. Mastrofski & James J. Willis, *Police Organization Continuity and Change: Into the Twenty-First Century,* 39 Crime & Just. 55, 124-125 (2010); Robert M. Bloom & Hillary Massey, *Accounting for Federalism in State Courts: Exclusion of Evidence Obtained Lawfully by Federal Agents,* U. Colo. L. Rev. 381, 397 (2008). *But see* Dafna Linzer, *In New York, A Turf War in the Battle against Terrorism,* Washington Post (March 22, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/21/AR2008032102980.html.

[178]*See, e.g.,* Joe Davidson, *Drug Cartels Corrupting U.S. Law Enforcement,* Washington Post B4 (June 9, 2011), 2011 WL 11478665; Statement of Chuck Grassley before the Senate Judiciary Committee, Congressional Testimony (November 19, 2009), 2009 WL 23324341.

[179]*See, e.g.,* U.S. Government Accountability Office, Law Enforcement Coordination 8 (April 2011), http://www.gao.gov/new.items/d11314.pdf (one-third of agents surveyed e "have gotten into turf wars with other federal law enforcement agencies during the course of an investigation during the past five years"). For more on the evolution and current state of federal agency conflicts, *see* Kirstin M. Finklea, *The Interplay of Borders: Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement* 19-25, Congressional Research Service (July 29, 2011), http://www.fas.org/sgp/crs/misc/R41927.pdf.

[180]Kirstin M. Finklea, *The Interplay of Borders: Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, supra* note 179 at 21.

[181]*See supra* note 173 & accompanying text.

defer to the Sheriff, because his office has stronger ties to that location and the victim. That calculus does not come into play at the federal level because, as I noted earlier, the federal law enforcement agencies listed above all have national jurisdiction. This, as noted above, means their turf is not linked to a specific state, county, city or other area. The agents employed by these agencies operate out of specific, geographically located offices,[182] but this is a matter of operational efficiency and, as such, does not define the legitimate scope of an agency's operations. That is a function of "operational turf," that is, of the statutes that define a given agency's investigative authority.[183]

If these statutes parsed investigative authority out among the five agencies listed above in a fashion analogous to how combat jurisdiction is parsed out among the five military branches, this would go a long way toward reducing the turf wars that currently plague federal law enforcement. Unfortunately, the statutes rarely do this, which means agencies often have overlapping investigative jurisdiction, which "can open the doors" to turf battles.[184] In a 2011 investigation of jurisdictional overlap among federal agencies, many agents reported that they had encountered uncertainty and disagreements about the appropriate allocation of investigative authority and said these disagreements often negatively affected investigations.[185] The 2011 report found that criminals' increasing use of cyberspace is only exacerbating the difficulties federal agents already face.[186]

While turf wars and overlapping or uncertain investigative jurisdiction continue to impede U.S. law enforcement's ability to respond to crimes, they are not the only factors that are eroding its ability to respond to cyber-threats. The problem law enforcement must confront is the civilian correlate of the problem General Alexander faces:[187] We can no longer assume that attacks which appear to constitute "mere" cybercrime are just that, i.e., are carried out by civilians who are "in" the United States and whose motives are

---

[182]*See, e.g.*, Federal Bureau of Investigation, Today's FBI 2010-2011 5, http://www.fbi.gov/stats-services/publications/facts-and-figures-2010-2011/facts-and-figures-2010-2011-pdf. *See also* Federal Bureau of Investigation, The FBI: A Centennial History 1908-2008 108, 118 (2008), http://www.fbi.gov/about-us/history/a-centennial-history/the-fbi-a-centennial-history-1908-2008 (noting that field offices collaborated in investigations of crime spanning wider geographic areas).

[183]*See* Kirstin M. Finklea, *The Interplay of Borders: Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, supra* note 179 at 21.

[184]*Id. See, e.g., See, e.g.,* U.S. Government Accountability Office, Law Enforcement Coordination, *supra* note 179 at 4 ("in a drug investigation involving a suspect who may be illegally procuring a large cache of firearms to protect the drugs, the FBI and DEA, which both have jurisdiction over illegal drugs, as well as ATF, which is responsible for regulating firearms, may be involved").

[185]*See id.*

[186]*See* Kirstin M. Finklea, *The Interplay of Borders: Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement, supra* note 179 at 37.

[187]*See supra* § III(A)(2).

purely personal.[188] An attack on a financial institution might be a cybercrime committed by a greedy U.S. citizen "in" the United States, but it might, instead, be (i) a cybercrime committed by a non-U.S. citizen operating from abroad or (ii) a cyber-sortie carried out by a hostile nation-state's own cyber command.[189]

If the attack hypothesized above constitutes domestic cybercrime committed by a U.S. citizen, it clearly falls within U.S. law enforcement's investigative authority under the bifurcated approach outlined above.[190] And the same is true if the attack constitutes transnational cybercrime carried out by a non-citizen; as a practical matter, investigating this type of cybercrime involves challenges law enforcement officers do not confront in purely domestic investigations,[191] but it is still their default responsibility.[192]

The truly problematic scenario is the one in which the attack is carried out by a hostile state's military hackers. This scenario is problematic for several reasons, the first and perhaps most critical of which is that the bifurcated approach assumes the nature of an attack is apparent.[193] As we saw earlier, it assumes this because in real-space there are certain "markers" that immediately differentiate an act of war from crime/terrorism.[194] As we also saw, those markers do not (necessarily) exist in cyberspace: Bits and bytes

---

[188]*See supra* § II(B).

[189]*See, e.g.,* John Leyden, *Leaked U.S. Cables Finger Chinese Army Hackers for Cyber-Spying,* The Register (April 18, 2011), http://www.theregister.co.uk/2011/04/18/byzantine_hades_cyber_espionage/. The attack hypothesized above could also constitute (i) non-nation-state-sponsored terrorism, which would clearly be a matter within law enforcement's investigative authority; (ii) nation-state-sponsored terrorism, which might be a matter for law enforcement but might also be considered an act of war to be dealt with by the military; or (iii) nation-state-sponsored crime, which would presumably be within law enforcement's investigative authority. See*, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* 20 at 423; Michael J. Robbat, *Resolving the Legal Issues Involving the Use of Information Warfare in the International Forum,* 6 B.U. J. Sci. & Tech. L. 10, 63 (2000). *See also* Susan W. Brenner & Anthony C. Crescenzi, *State-Sponsored Crime: The Futility of the Economic Espionage Act,* 28 Hous. J. Int'l L. 389 (2006).

[190]*See supra* §§ II(A) & II(B).

[191]*See, e.g.,* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime,* 20 J. Marshall J. Computer & Info. L. 347 (2002).

[192]*See supra* §§ II(A) & II(B).

[193]*See supra* §§ II(A) & II(B).

[194]*See supra* §§ II(A) & II(B). As we saw earlier one of the markers is that the attack is directed at a military target. *See id.* The 1941 attack that brought the United States into World War II was directed at a U.S. naval base, i.e., Pearl Harbor. *See, e.g.,* "Attack on Pearl Harbor," Wikipedia, http://en.wikipedia.org/wiki/Attack_on_Pearl_Harbor.

do not arrive bearing national insignia nor do they constitute weaponry that only nation-states can employ.[195] The bits and bytes used to launch a cyberwar attack of the type we are hypothesizing would begin their voyage to their U.S. target from a location outside the territorial United States but, as we have seen,[196] that, in and of itself, is not enough to reliably support the inference that an attack is an act of war.

Since cybercrime routinely originates from outside U.S. territory, it would be quite reasonable for U.S. law enforcement officers to assume an attack is crime, rather than war.[197] This would be their default assumption, and there is nothing in the attack we are hypothesizing that would bring it to the attention of the military.[198] The U.S. military has for decades monitored geographical vectors (i.e., U.S. airspace and coastal waters) for signs of a conventional attack, but the military does not, and cannot, monitor cyberspace in an effort to ascertain when what is ostensibly cybercrime is actually cyberwarfare.[199] If it were to do so, the U.S. military would invade what has historically and doctrinally been law enforcement's exclusive sphere of operations.[200]

This creates an opportunity for surreptitious war: A hostile state could use cyberspace to launch attacks that were designed to undermine the stability and viability of the United States,[201] but disguise the nature of the attacks by having them originate from a locale with no military associations and utilize tools and technology associated with civilians, perhaps with cybercriminals.[202] If a state were to do this (and for all we know, one already has),[203] U.S. law enforcement officers would construe the attacks as

---

[195]*See supra* § II(B).

[196]*See supra* §§ II(A) & II(B).

[197]Aside from anything else, the fact that the attack targets a civilian entity inferentially suggests it is crime, not war. *See supra* §§ II(A) & II(B).

[198]*See supra* note 197.

[199]*See, e.g.,* Aliya Sternstein, *Congress, Administration Grapple with Cyber Defense Authority,* NextGov.com (April 11, 2011), 2011 WLNR 8351086 (General Alexander confirmed "that the U.S. Cyber Command cannot monitor civilian networks").

[200]*See supra* § II(B).

[201]The attacks might, for example, target the U.S. financial system, in an attempt to destabilize the nation's economy. *See, e.g.,* Kevin Coleman, *Russia's Cyber Forces,* DefenseTech (May 27, 2008), http://defensetech.org/2008/05/27/russias-cyber-forces/ (cyberwar tactics include "disrupt[ing] financial markets" and "weaken[ing] the economy of their adversary"). *See also* Charles Arthur, *Nation-State Behind Major Cyber-attack on IMF, Say Experts,* The Guardian (June 13, 2011), 2011 WLNR 11740549 (cyberwar "waged by governments for economic . . . purposes").

[202]*See supra* § II(B). Estonia may have been the target of a similar attack in 2007. *See, e.g.,* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law,* 27 Berkeley J. Int'l L. 192, 205-206 (2009).

[203]*See supra* note 202.

cybercrime and do their best to respond, presumably after the fact.[204] If the response came after the attacks ended, then they would have inflicted the intended damage and the U.S. officers would be left with the essentially futile task of trying to track down and apprehend the perpetrators.[205] The foray into online war would have succeeded at basically no cost to the responsible state, and the United States might never realize it had been the target of a military attack.[206]

All of this has serious implications for the country's security: The U.S. military has been, and is, responsible for protecting the United States from externally-based attacks that threaten the social and economic viability of the country. The military's mission, though, is limited to protecting the country from demonstrable acts of war, i.e., from external attacks that can be attributed to a hostile nation-state and that involve the use of traditional military force. The military consequently has no authority to respond to external attacks that (i) cannot be reliability attributed to a hostile nation-state and/or (ii) only involve the use of cyberspace.[207]

This leaves law enforcement, which has historically responded to internal attacks involving citizen-on-citizen victimization.[208] As we saw above,[209] U.S. law enforcement now finds it increasingly necessary to respond to external attacks that involve the online victimization of U.S. citizens by non-U.S. citizens. Since these attacks involve individual-on-individual victimization and since the perpetrators' motives and the "harms" they inflict

---

[204]*See supra* note 86. If the attacks were large-scale in nature, the architects of the attacks could further conceal their true nature by making them appear to be discrete, unrelated attacks on targets in various parts of the country. Our hypothesized attackers might be able to exploit the highly segmented nature of state and local law enforcement to their advantage, by convincing officers in various geographical areas that they were dealing with different perpetrators in each instance. Aside from anything else, that would enhance the attackers' ability to disguise the event as a series of cybercrimes.

[205]*See, e.g.,* Scott Charney, *The Internet, Law Enforcement and Security,* Practicing Law Institute, 662 PLI/Pat 937, 945 (2001): "[W]hat . . . if law enforcement spends months investigating a `cybercrime' only to find another country is engaging in . . . information warfare? . . . [I]t would be like sending the FBI to Hawaii on December 7, 1941 to investigate a trespass by Japan."

[206]*See, e.g.,* Eneken Tikk, et al., Cyber Attacks against Georgia: Legal Lessons Learned 13, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia (November 2008), http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf (researchers investigating 2008 Georgia attacks were "unable to find" evidence of "state organisations guiding or directing attacks" either "because there was none . . . or because involvement by state organisations was conducted in a way to purposefully avoid attribution").

[207]*See supra* note 159. *See also* Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F. L. Rev. 121, 144-148 (2009) (cyberattacks do not qualify as acts of war under current laws of warfare).

[208]*See supra* § II(A).

[209]*See supra* § II(B).

fall within existing principles of criminal liability, the investigation of the attacks clearly fits within U.S. law enforcement's investigative authority. [210]

As a practical matter, U.S. law enforcement officers cannot effectively investigate all or even a substantial portion of the transnational cybercrime attacks that target U.S. citizens. This is in part attributable to the fact that cybercrime -- both transnational and domestic -- represents a new quantum of criminal activity that is added to the traditional criminal activity to which U.S. officers must continue to respond. It is also attributable to the fact that the processes of enforcing criminal law and bringing criminals to justice are linked to the territorially-based authority of a specific nation-state; law enforcement officers, courts and others involved in these systems legitimately operate only within the territory their sovereign controls.[211] There are processes by which U.S. law enforcement officers can obtain evidence from abroad, but they are complex, uncertain and move at a glacial pace.[212] This circumstance and the incremental burden cybercrime creates for officers who must still respond to traditional crimes combine to limit the extent to which U.S. law enforcement officers can pursue offshore-cybercriminals.[213] And this *de facto* limitation on their ability to investigate external attacks that appear to be cybercrime can create opportunities for the type of surreptitious warfare outlined above.[214]

Our commitment to the bifurcated, military-law enforcement approach to threat-control makes it difficult for the United States to address this vulnerability. We cannot, for a variety of reasons, simply expand the investigative authority of state, local and/or federal law enforcement officers so that their investigative authority extends outside the territorial boundaries of the United States. Aside from anything else, that would violate the territorial sovereignty of the countries in which they exercised this authority.[215]

---

[210]*See supra* § II(B).

[211]*See, e.g.,* Susan W. Brenner, Cyber-threats, *supra* note 8 at 201-222.

[212]*See* Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace 142-148 (2010).

[213]*See, e.g.,* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 80-81.

[214]McAfee's 2011 outing of "Operation Shady Rat," a five-year series of cyberattacks on corporate and government targets, illustrates how difficult it can be to determine whether an attack is mere cybercrime or something more. *Compare* Jim Finkle, *"State Actor" Behind Slew of Cyber Attacks,* Reuters (August 3, 2011), http://www.reuters.com/article/2011/08/03/us-cyberattacks-idUSTRE7720HU20110803?feedType=RSS&feedName=topNews&rpc=71 *with* Gabriel Perna, *McAfee's Rivals Scoff at Shady RAT Report,* International Business Times (August 5, 2011), http://www.ibtimes.com/articles/193338/20110805/mcafee-rivals-scoff-shady-rat-kaspersky-symantec.htm.

[215]*See, e.g.,* Restatement (Third) of the Foreign Relations Law of the United States §§ 432(2) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state"). *See also id.* at § 432 cmt. b, & 433 (1987); U.S. Department of Justice, Criminal Resource Manual § 267, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00267.htm.

And while the military's mission specifically encompasses extraterritorial threat response, we cannot, as noted above,[216] involve the U.S. military in responding to cyber attacks the provenance of which is uncertain. The military's mission is to respond to a verified military attack or deter such an attack. It is not an investigative entity, as such, and is therefore not qualified to pursue and apprehend cyber-perpetrators who would be brought back to the United States and interrogated as to the nature of a particular attack. And if U.S. military personnel were to invade another sovereign's territory in an effort to ascertain the nature and source of cyberattacks targeting the United States and/or to apprehend the perpetrator(s) of such attacks, that would constitute an act of war, though the cyberattacks themselves would not.[217]

This is an obviously untenable state of affairs, which is why in 2010 legislation was introduced into Congress that would add another element into the threat-control dynamic: civilian participation. We will examine that legislation in the next section.

C. Civilians

The first section below examines several U.S. legislative proposals that are designed to incorporate civilians into a cyber-threat response effort. The next section analyzes the conceptual issues raised by these proposals.

1. Legislative proposals

In 2010, several bills designed to improve the United States' ability to protect itself from cyberattacks were introduced in Congress.[218] One of them -- the Protecting Cyberspace as a National Asset Act of 2010 ["Protecting Cyberspace"] -- was introduced by Senators Lieberman, Collins and Carper.[219] The Senators said the bill was intended to remedy the "`disjointed and uncoordinated'" approach to cybersecurity that prevailed at the federal level by creating "`a public/private partnership to promote national cyber security" and "prevent and respond to cyber attacks.'"[220] Among other things, it created

---

[216]*See supra* note 207 & accompanying text.

[217]See supra note 159 & accompanying text.

[218]*See, e.g., Senate Bill Proposes Office of Cyberspace Policy,* CommWeb News (June 14, 2010), 2010 WLNR 12128815 (Lieberman-Collins-Carper, Kerry and Rockefelleer-Snowe bills in the Senate, Lipinski bill in the House).

[219]*See, e.g.,* Emelie Rutherford, *Senate Committee Oks Cybersecurity Bill on Majority Leader's Radar,* Defense Daily (June 25, 2010), 2010 WLNR 14036808.

[220]*Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses,* Senate Committee on Homeland Security & Governmental Affairs (June 10, 2010), http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=227d9e1e-5056-8059-765f-2239d301fb7f (quoting Senator Collins).

the National Center for Cybersecurity and Communications [NCCC] and made the NCCC's Director responsible for "working cooperatively with the private sector" to "lead the Federal effort to . . . protect, and ensure the resiliency of the Federal information infrastructure and national information infrastructure of the United States".[221]

The Protecting Cyberspace bill included what became controversial provisions concerning private sector entities that were part of the nation's "critical infrastructure."[222] The NCCC Director was required, "on a continuous . . . basis, [to] identify and evaluate the cyber vulnerabilities to covered critical infrastructure."[223] He or she was also required to issue regulations "establishing risk-based security performance requirements" for securing "covered critical infrastructure against cyber vulnerabilities through the adoption of security measures" that would satisfy requirements "identified by" the Director.[224]

The Protecting Cyberspace bill also made the NCCC Director responsible for ensuring that the "owners and operators of critical infrastructure" developed plans for responding to a "national cyber emergency."[225] And it authorized the President to declare such an emergency.[226] If a President declared a national cyber emergency, the owners and operators of critical infrastructure components were then required to implement their response plans and "develop and coordinate emergency measures or actions necessary to preserve the reliable operation, of covered critical infrastructure". [227]

---

[221]Protecting Cyberspace as a National Asset of 2010, S. 3480, § 242(f)(1)(A), http://www.opencongress.org/bill/111-s3480/text.

[222]*See id.* at § 248. The bill incorporated the definition of critical infrastructure contained in 42 U.S. Code § 5195c(e), i.e., "systems and assets, whether physical or virtual," that are "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[223]Protecting Cyberspace as a National Asset of 2010, *supra* note 221 at § 248(a).

[224]*Id.* at § 248(b).

[225]*Id.* at § 248(b)(2)(C). A national cyber emergency is defined as "an actual or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a signify cant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure." Id at § 241(17). National information infrastructure is defined as information infrastructure that is "owned, operated, or controlled within or from the United States" and "that is "not owned, operated, controlled, or licensed for use by a Federal agency". Id at § 241(18). Information infrastructure is defined as "the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically". Id. at § 241(10).

[226]*Id.* at § 249(1).

[227]*Id.* at § 249(3)(A)-(B).

The Lieberman-Collins-Carper legislation also provided for the enforcement of these requirements. Each year, the owners and operators of critical infrastructure components were required to "certify in writing to the Director" that they had developed and implemented the security measures and response plans required by the Protecting Cyberspace bill.[228] If they did not comply with this requirement, the NCCC Director could order them to do so and could, if necessary, bring a civil suit to enforce such an order.[229] The Director was also authorized to evaluate the security measures and response plans submitted by those responsible for critical infrastructure components.[230]

The Protecting Cyberspace bill quickly became a source of controversy as various sources reported that it gave the President an "Internet `kill switch'" he or she could use to "`shut down or limit Internet traffic.'"[231] In an effort to address this concern, the three sponsors of the original bill introduced a revised version – now known as the Cybersecurity and Internet Freedom Act – in February of 2011.[232] Section 2(c) of the new bill says that "[n]otwithstanding any provision of this Act, . . . neither the President, the Director of the National Center for Cybersecurity and Communications, or any officer or employee of the United States Government shall have the authority to shut down the Internet."[233] Aside from adding that disclaimer and judicial review of the NCCC Director's determination that a particular entity constitutes critical infrastructure and is therefore required to implement the security and response measures outlined above, the new bill was essentially a clone of its predecessor.[234]

In May of 2011, the White House issued its own Cybersecurity Proposal, which included provisions directed at the private sector that were very similar to those outlined above.[235] The primary difference between the proposals is that the White House plan

---

[228]*Id.* at § 250(a)(1).

[229]*Id.* at § 250(a)(2).

[230]*Id.* at §§ 250(b) & 250(c).

[231]Declan McCullagh, *Senators Propose Granting President Emergency Internet Power,* CNET (June 10, 2010), http://news.cnet.com/8301-13578_3-20007418-38.html (quoting the Center for Democracy and Technology).

[232]*See, e.g.,* Declan McCullagh, *Internet "Kill Switch" Bill Gets a Makeover,* CNET (February 18, 2011), http://news.cnet.com/8301-31921_3-20033717-281.html.

[233]Cybersecurity and Internet Freedom Act of 2011, S. 413 § 2(c), http://thomas.loc.gov/cgi-bin/query/F?c112:1:./temp/~c112tL4lSa:e959:.

[234]Declan McCullagh, *Internet "Kill Switch" Bill Gets a Makeover, supra* note 232. The review, above, of the Protecting Cyberspace and Cybersecurity and Internet Freedom Acts is cursory, out of necessity. The Protecting Cyberspace bill is 197 pages, and the Cybersecurity and Internet Freedom Act bill is 221 pages. It is therefore neither possible, nor necessary, to analyze each in depth. Protecting Cyberspace as a National Asset of 2010, *supra* note 220; Cybersecurity and Internet Freedom Act of 2011, *supra* note 233.

[235]*See* Office of the White House, Cybersecurity Proposal (May 12, 2011), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-

makes the Secretary of Homeland Security responsible for developing and implementing a "national cybersecurity incident response plan" in collaboration with federal, state, local, territorial and tribal governments and private sector "owners and operators" of critical infrastructure.[236]

These, of course, were not the only proposals Washington generated in 2010 and 2011. In July of 2011, Senator McCain, who wanted to create a new cybersecurity committee, noted that federal cybersecurity legislation had so far "`been drafted by at least three committees and at least seven committees claim some jurisdiction over the issue.'"[237] He also pointed out that "the White House and the Energy, Commerce and Defense departments have all put forward separate initiatives on the subject."[238] McCain

---

Provisions-Related-to-Computer-Security-Full-Bill.pdf. The White House proposal also included proposed revisions to the Computer Fraud and Abuse Act and legislation that required notice of data breaches. *See id* at Law Enforcement Provisions Related to Computer Security & Data Breach Notification.

[236]*See id.* at Department of Homeland Cybersecurity Authority § 243(c)(9). While this provision only encompasses "critical information infrastructure," a subsequent section of the proposal allows the Secretary of Homeland Security to designate private entities as components of the nation's "critical infrastructure" and to develop and enforce plans for addressing and mitigating cybersecurity risks. *See id. at* Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act at §§ 2, 3, 4, 5 & 8. This portion of the White House plan uses the same definition of critical infrastructure as the legislation proposed by the Senators. *See id.* at § 10(2). *See also supra* note 222.

Although the White House proposal does not call for the creation of a National Center for Cybersecurity and Communications or some similar entity, it does require the Secretary of the Department of Homeland Security to "designate and maintain a center to serve as a focal point within the federal government for cybersecurity with responsibilities that include the protection of federal systems and critical information infrastructure and the coordination of cyber incident response". *See* Office of the White House, Cybersecurity Proposal, *supra* note 235 at Department of Homeland Cybersecurity Authority § 243(c)(5).

[237]Ben Pershing, *On Cybersecurity, Congress Can't Agree on Turf,* Washington Post (July 18, 2011), http://www.washingtonpost.com/politics/on-cybersecurity-congress-cant-agree-on-turf/2011/07/18/gIQACGCWMI_story.html (quoting Senator McCain).

[238]*Id.* In June of 2011, the Speaker of the House and the House Majority Leader announced "the formation of a new Cybersecurity Task Force", which would analyze cybersecurity issues and make recommendations to House Republican "leaders" in October, 2011. *See* Speaker Boehner & Leader Cantor Announce New Cybersecurity Task Force Led. By Rep. Thornberry, Speaker of the House (June 24, 2011), http://www.speaker.gov/News/DocumentSingle.aspx?DocumentID=248724. Also, Senator Harry Reid earlier introduced a bill that is designed to protect the U.S. from cyberattack. *See* S. 21: Cyber Security and American Cyber Competitiveness Act of 2011, http://www.govtrack.us/congress/bill.xpd?bill=s112-21. And in March of 2011, Congressman Jim Langevin introduced a bill to "significantly strengthen protections against dangerous cyber threats." *Langevin Introduces Bill to Strengthen Cybersecurity, Prevent Attacks*, U.S. Congressman Jim Langevin (March 16, 2011),

claimed his proposed Select Committee on Cyber Security and Electronic Leaks would "quell" the competition "`for cyber jurisdiction'" that had arisen among Congressional committees.[239] Senators Lieberman and Collins disagreed, saying it would be "`a waste of time to restart the process'" when their committee had already done so much work on the issue.[240] One commentator put the bickering, and the proliferation of cybersecurity committees and task forces, down to the fact that "lawmakers hate giving up turf."[241]

Aside from establishing that turf battles are not confined to federal and state agencies, the debate over McCain's committee demonstrated that lawmakers and law enforcers in Washington see cybersecurity as a matter of pressing concern that requires innovative solutions. It is the need for, and the complexity of developing, such solutions that accounts for the proliferation of efforts to that end and the fact that they have, so far, proven unproductive. Historically, when Congress has been confronted with the need to act quickly to address a traditional threat to national security, it has done so; in 2002, for example, it took less than a month to adopt a resolution responding to then-President Bush's request for authority to use military force against Iraq.[242] Congress has acted with similar expedition on the other occasions when it was called upon to approve a military response to an external threat.[243]

---

http://langevin.house.gov/news/press-releases/2011/03/langevin-introduces-bill-to-strengthen-cybersecurity-prevent-attacks.shtml.

For the Department of Energy's legislative cybersecurity efforts, *see, e.g.,* Statement of Patricia Hoffman, Assistant Secretary – Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy Before the Committee on Energy and Natural Resources of the U.S. Senate (May 5, 2011), http://www.doe.gov/sites/prod/files/ciprod/documents/Final_Testimony%2826%29.pdf. For the report of the Department of Commerce's task force on cybersecurity, *see* Cybersecurity, Innovation and the Internet Economy, The Department of Commerce Internet Policy Task Force (June 2011), http://www.nist.gov/itl/upload/Cybersecurity_GreenPaper_FinalVersion.pdf. I assume Senator McCain's reference to Department of Defense cybersecurity initiatives refers to the efforts examined in § III(A), *supra.*

[239]Marcus Weisgerber, *U.S. Senate Debates Cyber Oversight Proposal,* Defense News (July 19, 2011), http://www.defensenews.com/story.php?i=7135581&c=POL&s=TOP.

[240]Ben Pershing, *On Cybersecurity, Congress Can't Agree on Turf, supra* note 237 (quoting Senators Lieberman and Collins).

[241]*Id.*

[242]*See, e.g.,* "Iraq Resolution," Wikipedia, http://en.wikipedia.org/wiki/Iraq_Resolution.

[243]*See, e.g.,* "United States Declaration of War upon Japan," Wikipedia, http://en.wikipedia.org/wiki/United_States_declaration_of_war_upon_Japan (took Congress one day to declare war on Japan after the attack on Pearl Harbor); "American Entry into World War I," Wikipedia, http://en.wikipedia.org/wiki/American_entry_into_World_War_I#Declaration_of_war (Congress declared war on Germany four days after the President asked for such a declaration).

The problem Congress faces in dealing with cybersecurity is that, as we saw earlier, the internal-external threat dichotomy becomes meaningless when attacks are vectored through cyberspace. It is therefore difficult, even impossible, to ascertain with confidence whether an attack originated "outside" or "inside" the territorial United States. Cyberattacks are, as a result, insidious, pervasive and enigmatic.

They are insidious because, as we have seen, a computer that is linked to the Internet is vulnerable to infiltration or attack by online criminals, terrorists or warriors.[244] Cyberspace effectively makes every point on the globe coterminous with, or potentially coterminous with, the other points on the globe. Geographical space has ceased to be a source of security; the United States can no longer rely on natural barriers or man-made barriers such as NORAD[245] to detect and deflect cyberattacks from "outside." There is no "there" and "here," at least not insofar as those concepts have consequential import for a sovereign's ability to protect its territory, its citizens and its assets.

Cyberattacks are pervasive for a related reason, i.e., they do not (necessarily) differentiate between "sovereign" targets and "citizen" targets.[246] Cybercriminals attack individuals, private sector entities and governmental and military targets, and the same is, or is likely to be, true of cyberterrorists.[247] Conversely, it is already apparent that "civilians," as well as "sovereigns," will be the targets of cyberwarfare.[248] Since the notion of "inside" and "outside" threats, and the concomitant division of targets into "civilians" and "sovereign," becomes meaningless in cyberspace, it is no longer reasonable, or possible, to assume that each target category is vulnerable only to a corresponding type of attack, i.e., that civilians are only attacked by cybercriminals and cyberterrorists and that government entities are only attacked by nation-states. Each target category is now at least potentially vulnerable to the full range of cyber-threats, which, again, means the bifurcated approach to threat control is no longer adequate.[249]

Finally, cyberattacks are enigmatic because it can be difficult, if not impossible, to determine the geographical location from which an attack was launched and/or the identity/affiliation of the attacker(s).[250] This, as we saw above, further erodes the viability

---

[244]*See, e.g.,* Michael Joseph Gross, *Enter the Cyber-dragon*, 1 Vanity Fair (September 2011), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109#gotopage1.

[245]*See* North American Aerospace Defense Command, http://www.norad.mil/.

[246]*See supra* § II(B).

[247]*See supra* § II(B).

[248]*See supra* § II(B).

[249]*See supra* § II(B).

[250]*See supra* § II(B).

of the bifurcated approach,[251] all of which is why Congress, the White House and various government agencies want to bring civilians into the cyber-threat response process.[252]

But while civilian involvement is clearly an essential component of an effective cyber-threat response process, it is also a significant modification of how modern states approach internal and external security. Incorporating civilians into a state's cyber-threat process therefore raises both practical and conceptual issues. Our analysis, in the remainder of this section and in § IV, primarily focuses on the conceptual issues.[253]

2. Conceptual issues

It is clear from the proposals outlined above that the United States will have to resolve two conceptual issues before it can successfully integrate civilians into a blended internal-external cyber-threat response effort: One is "recruitment," i.e., the need for a process that legitimately incorporates civilians into such an effort. The other issue is "management," i.e., the need to structure and implement civilian participation in such an effort. We will examine recruitment in this section and take up management in § IV.

Recruitment may seem trivial or even irrelevant, but it is not. While efforts to incorporate civilians into a cybersecurity effort remain at a nascent stage, many entities are not enthusiastic about the measures outlined above. As one commentator noted, "private sector stakeholders have expressed concern that increased federal intervention in private cyber networks would impose excessive burdens and . . . stifle innovation and commerce."[254] Companies also fear that government-imposed cybersecurity standards and practices could "have adverse effects on the private sector's ability to parry cyber-attacks." [255] And some say "asking private industry to deal with cybersecurity [i]s like having the airlines deal with air attacks."[256]

---

[251]*See supra* § II(B).

[252]*See supra* § II(B). For more on why private sector involvement is essential for the United States' ability to protect itself from cyber-threats, *see, e.g., See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1024-1039.

[253]It focuses on the conceptual issues because a state must resolve them before it can embark on integrating civilians into its cyber-threat response effort. Once it resolves the conceptual issues, the state can tackle the practical issues.

[254]Richard Weitz, *Preventing the Next Private Sector Cyber Security Breach,* Second Line of Defense (July 18, 2011), http://www.sldinfo.com/preventing-the-next-private-sector-cyber-security-breach/. For similar views, see the letter Cisco Systems, IBM and the Oracle Corporation sent to Senators Lieberman and Collins: http://www.scribd.com/doc/34006241/Cisco-IBM-Oracle-letter-re-S-3480-06-24-10.

[255]Richard Weitz, *Preventing the Next Private Sector Cyber Security Breach, supra* note 254.

[256]John Eggerton, *WH Cybersecurity Coordinator: Privacy, Speech Protections Are Core Tenets,* Broadcasting & Cable (August 4, 2011),

The first two concerns seem to reflect businesses' normal reservations about "excessive" government regulation.[257] As such, they go less to the legitimacy of the "recruitment" process and more to the process of managing civilian participation in a cybersecurity effort.

The third concern, though, is different. It reflects an appreciation of an issue I have written about before, i.e., that involving civilians in a cybersecurity effort transforms them into . . . something else.[258] If such an effort focused only on cyberwar, their status would shift from noncombatant to combatant;[259] if it focused only on cybercrime and cyberterrorism, their status would shift from civilian to police officer.[260] In a blended cyber-war/crime/terrorism response effort, the shift is more generic. Civilians transform from nonparticipant into participant, which has several implications, the most obvious of which is that their role is no longer limited to performing civilian functions.

It also encompasses actively participating in the conduct of hostilities.[261] What, precisely, might that mean? As we saw earlier, the two cybersecurity bills and the White House's cybersecurity proposal all specify that civilian owners and operators of critical infrastructure components will be required to develop "response plans" and implement them if the President declares a national cyber-emergency.[262] As far as I can tell, neither of the bills nor the White House proposal explains what such a "response" entails.[263] It

---

http://www.broadcastingcable.com/article/471972-WH_Cybersecurity_Coordinator_Privacy_Speech_Protections_Are_Core_Tenets.php.

[257]*See, e.g.*, Committee on Capital Markets Regulation, Interim Report of the Committee on Capital Markets Regulation ix-xii (2006), http://www.capmktsreg.org/pdfs/11.30Committee_Interim_ReportREV2.pdf. *See also* Orion Corp. v. State, 109 Wash.2d 621, 648-649, 747 P.2d 1062, 1076-1077 (Wash. 1987).

[258]*See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1024-1039.

[259]*See id.* at 1015 (law of armed conflict distinguishes "between combatants (soldiers) and noncombatants(civilians)" and makes civilians "non-actors" who have no legitimate role in military hostilities).

[260]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 9 at 60-64 (development of police forces eliminated "civilian involvement" in crime/terrorism control and gave that task to professional law enforcement officers).

[261]*Id.* at 1048.

[262]*See supra* notes 225 - 227 & 234 & accompanying text. *See also* Cybersecurity and Internet Freedom Act of 2011, S. 413 §§ 248(b)(3) & 249(a)(3)(A), *supra* note 233; Office of the White House, Cybersecurity Proposal, *supra* note 235 at Department of Homeland Cybersecurity Authority §§ 243(c)(5)(B) & 243(c)(9)-(10).

[263]This is perhaps not surprising, given that in August of 2011 the Government Accountability Office "told Pentagon officials to define `cybersecurity' so the military

would certainly involve defensive measures, i.e., efforts to secure systems and withstand the effects of a hostile attack. But it could also encompass offensive measures, such as launching counter-cyber-strikes at an attacker; nothing in any of the proposals indicates this would be required of the civilians involved in cybersecurity, but the U.S. military has technologies that can launch offensive cyber-strikes.[264]

One could argue that participating in a purely defensive response is not enough to transform a civilian entity from cyber-noncombatant to cyber-combatant,[265] but even if we assume for the purposes of analysis that this view is doctrinally valid, I suspect it is also irrelevant. I, for one, do not believe a cyber-threat control effort of the type the Senators' bills and the White House's proposal seem to contemplate can be based primarily on having private sector entities, in effect, batten down their cyber-hatches and ride out a storm of cyberattacks. This might be a viable approach if Cyber Command and its constituent cyber commands could supplement this defensive tactic with offensive measures that repelled the attackers and ended the cyber-emergency, but I find this scenario equally problematic. For one thing, it assumes a stable, identifiable

---

services adopt the same terminology". Aliya Sternstein, *Auditors: Pentagon Budget Has Fuzzy Numbers,* NextGov (August 1, 2011), http://cybersecurityreport.nextgov.com/2011/08/auditors_pentagon_cyber_budget_has_fuzzy_numbers.php. *See also* Eric Chabrow, *GAO: Can DoD Keep Pace with Cyber Threats?,* GovInfoSecurity (July 25, 2011), http://www.govinfosecurity.com/articles.php?art_id=3892 (GAO criticized Defense Department for not having "uniformly defined" what "constitutes a cyberforce").

[264]*See, e.g.,* U.S. Secretary of the Air Force, Air Force Instruction 41-402: Legal Reviews of Weapons and Cyber Capabilities 5 (July 27, 2011), http://www.fas.org/irp/doddir/usaf/afi51-402.pdf (defining "cyber capability" as "any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities"). *But see* Aliya Sternstein, *Cybersecurity: Defense Department,* Government Executive (August 1, 2011), http://www.govexec.com/story_page.cfm?articleid=48408&oref=todaysnews (noting that the newly released Department of Defense cyber strategy focuses on defensive, rather than offensive, measures). On a related issue, the Defense Department has indicated that damage to U.S. critical infrastructure and/or injury to U.S. citizens can warrant the use of kinetic force in response. *See, e.g.,* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War,* Wall Street Journal (May 31, 2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

On a possibly related note, many U.S. companies have for years argued that they should be allowed to strike back at cybercriminals and other attackers. *See, e.g.,* Jeff Green, *Computer Users Need "Offensive" Security,* Security Takes the Offensive 3-4, 5-8, 27-30 McAfee (2010), http://www.mcafee.com/us/resources/reports/rp-security-journal-summer-2010.pdf. *See also* Bruce P. Smith, *Hacking, Poaching and Counterattacking: Digital Counterstrikes and the Contours of Self-Help,* 1 J.L. Econ. & Pol'y 171, 176-178 (2005).

[265]*Cf.* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1026-1035.

cyber-field of battle on which U.S. forces could confront, and defeat, an ascertainable unified opponent. As we saw earlier, that scenario, while not impossible, is unlikely.[266]

I also find this scenario problematic for another reason: I do not see how Cyber Command and its constituent cyber commands could possibly "defend" U.S. companies from a series of sustained cyber-attacks. Aside from anything else, I am not convinced that the various commands have the resources needed for such an endeavor;[267] there is also the fact that, as we saw earlier, Cyber Command has not developed policies and procedures that integrate the disparate commands into a unified entity.[268] But even if Cyber Command satisfactorily addresses these and other operational issues, I do not see how it, alone, could "defend" U.S. civilians from cyberattackers. As I noted above, cyber-threats, unlike their real-space counterparts, are insidious, pervasive and enigmatic which means a cyberattack almost certainly would not focus on an identifiable, stable battle-"space" and involve an ascertainable, unified opponent. And attacks would in all probability target systems operated by private entities, at least to some extent.

If the targeted entities' only response was to try to secure their systems and ride out the attacks, this would either (i) be the United States' *only* response to the attack or it (ii) would be up to Cyber Command and its constituent commands to take offensive measures against the attackers.[269] We will assume, for the purposes of analysis, that Cyber Command and the lesser commands are capable of, and do, implement such measures . . . but to what extent? I find it difficult to believe that Cyber Command and its constituent units would be able to launch an offensive response against every attack being waged on a U.S. company. Even if they were, the attackers could simply end that assault and move on to another target, which would mean that Cyber Command would eventually have to do the same . . . after it had ascertained which system(s) the attackers had moved on to.

I also see yet another complication: Would it be possible for Cyber Command to take effective offensive (and defensive) measures without being able to operate from within the attacked system and/or by utilizing resources of that system? In other words, if a private sector entity's computer systems were under attack, could Cyber Command protect the company without having access to its systems or, at a minimum, assistance

---

[266] *See supra* § II(B).

[267] *See, e.g.,* J. Nicholas Hoover, *Senate Confirms Military Cybersecurity Chief,* Information Week Government (May 11, 2010), http://www.informationweek.com/news/government/security/224701513 (noting that some "details of Cyber Command remain to be worked out, such as force size").

[268] *See supra* note 132 & accompanying text. *See also supra* note 263.

[269] The utility of adding an offensive cyber-response to the scenario is that by making the attack more risky, and perhaps more "expensive," for the attackers, it could cause them to terminate the attack sooner than they would otherwise. *See, e.g.,* Raoul Naroll, Vern L. Bullough & Frada Naroll, Military Deterrence in History 3-4 (1974).

from the employees who were in charge of those systems?[270] I suspect the answer will, at least in part, depend on the nature and circumstances of the attack.[271]

My point is that I do not believe U.S. companies will be able to rely solely on defensive measures in the event of a cyberattack. As opposed to the scenario above, which assumes a large-scale, coordinated attack (or series of attacks), I suspect it is far more likely that U.S. targets, both government and civilian, will come under periodic, sporadic attacks from unknown attackers, who may or may not persist from incident to incident. If the civilian sector's only role is to hunker down and try to ride out an attack, then certain attackers, most notably nation-states, could effectively impair the functioning of one or more sectors of the U.S. economy simply by attacking the entities involved in those sectors. The attacks would, at least to some extent, impair their ability to conduct business as usual, which could be the attackers' objective.

It seems, then, that civilians need to be part of a cyber-response effort and that their role may well encompass offensive, as well as defensive, measures. The person who analogized "asking private industry to deal with cybersecurity" to "having the airlines deal with air attacks"[272] clearly recognized that this is an implicit element of the current cybersecurity proposals. It is not surprising that he/she found this result unacceptable. It is likely others have reacted similarly because, as I explain elsewhere, for at least a century civilians have had no responsibility for maintaining internal or external order (unless they join the military or law enforcement).[273] In the preceding centuries, civilians bore most, if not all, of the responsibility for ensuring their societies were protected from

[270]If the employees of such a company actively assisted Cyber Command personnel who were responding to an attack, the civilians' status could shift from that of noncombatant to combatant. *See, e.g.,* Jennifer S. Martin, *Adapting U.C.C. § 2-615 Excuse for Civilian-Military Contractors in Wartime*, 61 Fla. L. Rev. 99, 138 (2009).

[271]If the attack is purely external, e.g., if it is a distributed denial of service (DDoS) attack that bombards the company with traffic in an effort to knock it offline, Cyber Command might well be able to respond without having access to the company's own systems. *See, e.g.,* "Denial-of-service attack," Wikipedia, http://en.wikipedia.org/wiki/Denial-of-service_attack. If, on the other hand, the attack involves the infiltration of the company's system by, say, malware or hacking, Cyber Command might need access to the system or the cooperation of the company's information security staff to deal with it. *See, e.g.,* "Stuxnet," Wikipedia, http://en.wikipedia.org/wiki/Stuxnet.

[272]*See supra* note 256 & accompanying text.

[273]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 60-65. *See also* Susan W. Brenner, Cyber Threats, *supra* note 8 at 15-16, 165 -169, 213-215; Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1073-1075.

both internal and external threats.[274] We have forgotten that; we assume security is a matter that is to be, and will be, dealt with by the appropriate professionals.[275]

The Senators' bills and the White House's proposal recognize that while this state of affairs may continue to prevail in real-space, the responsibility for dealing with threats in cyberspace must be shared by the military, law enforcement and at least some of the civilian population.[276] If nothing else, this is evident from how Howard Schmidt, the White House's "Cyber Czar,"[277] responded to the air-attack/cyberattack analogy: He said "building security into systems has become a business imperative"; and he noted that the government needs to "help" those who do not realize this to "understand they have that shared responsibility."[278] Schmidt might more accurately have said that the

---

[274]*See, e.g.,* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 60-65; Susan W. Brenner, Cyber Threats, *supra* note 8 at 15-16, 165 -169, 213-215.

[275]*See* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 65-76. Indeed, our laws reinforce that. If someone responds to a crime by conducting their own investigation, they will be prosecuted, essentially for vigilantism. *See, e.g.,* Steven v. Hernandez, 2007 WL 2238657 *1, *5 - *11 (S.D. Cal. 2007); State v. Emmons, 141 N.M. 875, 880, 161 P.3d 920, 926 (N.M. App. 2007). And as noted earlier, if a civilian engages in military combat, his/her status changes from noncombatant to unlawful combatant. *See supra* notes 89 & 254.

[276]*See, e.g.,* Statements on Introduced Bills and Joint Resolutions, Congressional Record 157 Cong. Rec. S872-01, S911, 2011 WL 556892 (February 17, 2011), (statement of Senator Lieberman regarding the Protecting Cyberspace and Internet Freedom Act of 2011) (noting that the "private sector is also under attack" in cyberspace). *See also id*.:

> The United States requires a comprehensive cyber security strategy backed by effective implementation of innovative security measures. There must be strong coordination among law enforcement, intelligence agencies, the military, and the private sector owners and operators of critical infrastructure.

[277]*See, e.g.,* Andy Greenberg, *Finally, A Cyber Czar,* Forbes (December 21, 2009), http://www.forbes.com/2009/12/21/cyber-czar-named-security-business-in-the-beltway-schmidt.html.

[278]John Eggerton, *WH Cybersecurity Coordinator: Privacy, Speech Protections Are Core Tenets,* Broadcasting & Cable (August 4, 2011), http://www.broadcastingcable.com/article/471972-WH_Cybersecurity_Coordinator_Privacy_Speech_Protections_Are_Core_Tenets.php. It is also evident from the fact that all of the government's Cyber Storm cybersecurity exercises have involved private sector entities working with state and federal agencies in responding to cyberattack scenarios. *See, e.g.,* Cyber Storm: Securing Cyberspace, U.S. Department of Homeland Security, http://www.dhs.gov/files/training/gc_1204738275985.shtm.

government needs to "help" these people "understand that they *now* have that shared responsibility."

This is the problem of recruitment. In real-space, at least in the United States, recruitment is voluntary: We no longer have a draft; those who are so inclined volunteer to serve in the military.[279] And law enforcement agencies hire officers from candidates who voluntarily apply for those positions.[280] The rest of us assume that security (and, by extension, cybersecurity) is the province of those who have chosen to engage in the processes of protecting the rest of us from hostile military forces, criminals and terrorists.

We are therefore not inclined to "get involved" in security (or cybersecurity). This disinclination is the product of a culture and a legal system that discourage citizens from participating in law enforcement and/or military combat on the quite logical premise that untrained civilians are only likely to impede trained professionals in the performance of their duties.[281] In real-space security, the concern that involving lay civilians in such activity could have a significant downside is exacerbated by the fact that both law enforcement and military combat involve the use of physical violence.

That factor does not apply, or at least does not apply to the same extent, when the issue is civilian involvement in cybersecurity. But this scenario has its own issues. One, as noted above, is the so-far prevalent disinclination of civilians to become involved in any type of security effort. That disinclination will have to be overcome if civilians, and civilian-owned entities, are to be successfully recruited into a cybersecurity effort. But

---

[279]*See, e.g.,* "Conscription in the United States," Wikipedia, http://en.wikipedia.org/wiki/Conscription_in_the_United_States.

[280]*See, e.g.,* Welcome to the Police Recruitment and Retention Clearinghouse, RAND, http://www.rand.org/ise/centers/quality_policing/cops.html.

[281]*See, e.g.,* Williams v. Tharp, 914 N.E.2d 756, 765 (Ind. 2009) (best to leave the task of investigating potential criminal activity and deciding "upon the appropriate response to trained professionals"). *See also supra* note 275.

The disinclination to get involved can, as one article noted, also be a product of "ignorance" and "denial:"

> Google executives reportedly believed that the American government monitors this country's Internet infrastructure the same way it monitors foreign military threats to keep the geographic homeland secure. A former White House official told me, "After Google got hacked, they called the N.S.A. in and said, 'You were supposed to protect us from this!' The N.S.A. guys just about fell out of their chairs. They could not believe how naïve the Google guys had been.

Michael Joseph Gross, *Enter the Cyber-Dragon, supra* 244 at 5. This article also suggests that at least some of the U.S. corporate sector's disinclination to take responsibility for cybersecurity is the result of companies not sharing information about the cyberattacks they have sustained. *See id.* at 11 ("`top corporate managers -- following the advice of their lawyers -- are reflexively keeping breach information secret from other companies that are trying to defend themselves'").

overcoming the disinclination is a delicate, difficult matter for the leaders of the United States or, for that matter, for any country: They would have to convince the populace that the government cannot protect them, and their assets, from cyber-threats while, at the same time, maintaining civilian confidence in the government's ability to protect them from other threats.[282]

There is another downside for the private sector entities affected by the new cybersecurity proposals: the cost of the hardware, software and expertise they will need to maintain the requisite level of security. As we saw, the Senators' bills and the White House's proposal require entities that are part of the nation's critical infrastructure to develop and implement security measures and plans for responding to a national cyber-emergency.[283] The entities must certify, every year, that they have measures and plans in place that are adequate to face the risks they confront; their certifications are subject to review by the official who is assigned responsibility for implementing this part of the proposed cybersecurity initiative.[284]

This means the companies will bear the costs of implementing these measures; there is no provision in any of the proposals that would reimburse affected private sector entities for the expense involved in implementing the required security measures.[285] This

---

[282]One article describes the prevailing corporate attitude as follows:

> `What are the subconscious assumptions that companies bring to the issue of foreign cyber-attacks on their networks?,' a senior Senate staffer who works on cyber-issues asked. . . . `They assume that if something bad happens government will take care of the losses. They act like they don't really believe that a bank could get completely taken out, or that a tech giant could get its whole lunch eaten. . . .'

Michael Joseph Gross, *Enter the Cyber-Dragon, supra* 244 at 12.
I suspect we will see the disinclination eroded gradually, as news outlets and other media publicize leaked information about cyberattacks and, in so doing, begin to cultivate attitudes similar to those that have driven many citizens to invest in alarm systems and burglar bars.

[283]*See supra* notes 225-230 & 234 & 236 & accompanying text.

[284]*See, e.g.,* Cybersecurity and Internet Freedom Act of 2011, S. 413 § 250(a)-(b), *supra* note 233.

[285]And this is likely to exacerbate an attitude that prevails in some companies, i.e., the tendency to doubt the return on investment of money spent on cybersecurity. *See, e.g.,* Bill Brenner, *Companies on IT Spending: Where's the ROI?,* CSO (January 25, 2010), http://www.csoonline.com/article/518764/companies-on-it-security-spending-where-s-the-roi-. An article on cyber-war described a far from atypical exchange between a corporate officer and the company's information security personnel:

> One . . . security specialist recalls a conversation with a chief financial officer and a chief information officer of a major corporation after finding

will only exacerbate the general disinclination companies, like other civilians, have with regard to involving themselves in cybersecurity.

And all of that creates the challenge of recruitment. In § IV, we will analyze the approach the U.S. government is using in an effort to recruit civilian-owned entities into a cybersecurity effort and then examine a possible alternative approach, an extrapolation from certain historical practices.

IV. The Limits of Bureaucratic Control . . .

> *[`T]he old structures . . . -- state, non-state, . . . private -- . . . break down [in cyberspace*].[286]

In the remainder of this article, I assume, for the reasons outlined above, that civilian participation is an essential element of an adequate, effective U.S. cybersecurity initiative. The focus of the analysis below is therefore not on whether such participation is warranted but is, instead, on how it might best be achieved.

This section analyzes the approach the U.S. government is relying on to develop an adequate, effective cybersecurity initiative, i.e., the efforts reviewed in § III, *supra.* As noted earlier,[287]these efforts commendably focus on remediating factors that contribute to the inefficacy with which existing U.S. threat-control structures confront cyber-threats. The problem, as I explain below, is that while the efforts are commendable, they are also inadequate because they attempt to "update" bureaucratic systems that were developed to control threats that are simpler and more parochial than the ones we now confront.[288]

> 65 vulnerabilities in the company's networks. . . . `What's the worst that can happen if we don't fix any of these?' the C.F.O. asked.
>
> `We have large exposure,' answered the C.I.O. `We could potentially be attacked –'
> `No, no, no. What is the financial impact if we don't do any of these?'
> `We're not regulated or audited, so there won't be any fines.'
> The C.F.O. answered, `You get no budget,' and the topic was closed.

Michael Joseph Gross, *Enter the Cyber-Dragon, supra* 244 at 9-10.

[286]*Id*. at 11 (quoting General Michael Hayden, former director of the N.S.A and of the C.I.A.)

[287]*See supra* § II.

[288]*See supra* §§ II & III. General Hayden, who was quoted above, seems to agree, at least to some extent. *See supra* note 286. While participating in a panel discussion in the summer of 2011, he said

> `[w]e may come to a point where . . . what is permitted there is something that we would never let the private sector do in physical space,' he said.

Section IV(A) puts these efforts into context by (i) tracing the U.S. government's increasing reliance on bureaucracy and (ii) examining the historical and other factors that shaped Weber's views on bureaucracy. Section IV(B) then analyzes the efficacy of the efforts outlined in § III, *supra* and finds them wanting. Section V outlines a possible alternative, an approach that is based on an older, more decentralized approach to maintaining internal and external order.

A. Business as Usual

> *Once it is fully established bureaucracy is among those social structures which are the hardest to destroy.*[289]

The efforts outlined in § III are all predicated on the bureaucratic model that has come to dominate governance in the United States and elsewhere (and also plays a significant role in the private sector).[290] We have become accustomed to bureaucracy; it has, in effect, become "business as usual."

In this section, we will engage in a rather modest exercise in the sociology of knowledge by approaching bureaucracy as a problematic construct. The sociology of knowledge is essentially concerned with the "social construction of reality," i.e., with how the orchestrations human beings develop and then rely upon to order their relationships with each other become perceived as having an objective reality.[291] This can occur in various ways, one of which involves the process of institutionalization.[292]

Institutionalization begins with habitualization: with the development of patterns of human activity that become routinized and are eventually "legitimated."[293] Legitimation

---

> `. . . [H]ow about a digital Blackwater?' he asked.`. . . [W]e have privatized certain defense activities . . . and now you've got a new domain in which we don't have any paths trampled down in the forest in terms of what it is we expect the government . . . to do.'

Andrew Nusca, *Hayden: "Digital Blackwater" May Be Necessary for Private Sector to Fight Cyber Threats,* ZD Net (August 1, 2011), http://www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/53639.

[289]From Max Weber: Essays in Sociology 228 (H. Gerth & C. Mills, trans. and eds. 1958).

[290]*See supra* note 5.

[291]*See, e.g.,* Peter Berger & Thomas Luckmann, The Social Construction of Reality: A Treatise in the Sociology of Knowledge 1-3, 89 (1966). The processes by which social phenomena become perceived as objective phenomena that exist separately and independently of human activity is known as reification. *See id.* at 89.

[292]*See id.* at 51-92.

[293]*See id. See also id.* at 92-104 (legitimation).

is the process by which a newly developed institution is "`explained'" and justified, i.e., by which it becomes accepted as a legitimate and even inevitable element of a social system.[294] Once this process has taken place, we will perceive the institution as a "facticity, an *opus alienum* over which" we have "no control rather than as the *opus proprium* of" our "own productive activity."[295] In other words, we forget we created the institution for purely practical purposes and come to regard it as an entity that exists independently of us. This reification of institutions can result in a society's persisting in routinized behaviors that have ceased to be productive and, indeed, may have become counterproductive.[296]

That brings us to our sociology of knowledge exercise, which will proceed in two stages: In the remainder of this section, we will examine the rise of bureaucracy in the United States and the historical context in which Max Weber developed his views on bureaucracy. In the next section, we analyze the role bureaucracies are playing in the United States' efforts to develop an effective cyber-threat control structure and consider whether the bureaucratic model of organization advances, or impedes, this process.

As one author noted, "[d]uring its first 150 years, the American republic was not thought to have a `bureaucracy,'" but by 1925 "nearly half a million" people worked for government agencies.[297] The New Deal and World War II only exacerbated the earlier increases in the size of U.S. government bureaucracies, a phenomenon due in large part to the rise of regulatory agencies at both the state and federal levels.[298] As one observer

---

[294]*See id.* at 61. *See also id.* at 92-104.

[295]*Id.* at 89.

[296]*See supra* note 291. This can, of course, be true of bureaucracy: As an "anonymous White House aide" noted in a memo written during the Vietnam war, bureaucracy "`tends to contort policy to existing structures rather than adjusting structures to reflect changes in policy.'" Robert W. Komer, Bureaucracy at War: U.S. Performance in the Vietnam Conflict 17 (1986). *See also* James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 98 ("Any organization, and *afortiori* any public organization, develops a genuine belief in the rightness of its mission").

[297]James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 77. *See also id.* at 87-90 (tracing developing of federal and state bureaucracies).

[298]*See, e.g.,* Arianne Renan Barzilay, *Women at Work: Toward an Inclusive Narrative of the Rise of the Regulatory State,* 31 Harv. J.L. & Gender 169, 172-173 (2008); James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 78. *See also* Larry Gerber, *World War II and the Expansion of Government in America*, 75 National Forum 30 (No. 4) (1995); Cass R. Sunstein, *Constitutionalism after the New Deal*, 101 Harv. L. Rev. 421, 421-422, 459 (1987).

James Q. Wilson ascribes much of the growth in American bureaucracy to "bureaucratic clientelism," i.e., to the development of clientele-oriented departments" that arose to address the "distinctive interests" that were the product of a "diversifying economy." James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 87-91. He also attributes it to the development of federal grants to state and local governments, which

notes, the "growth in the size" of bureaucracy can to a great extent be explained by the need for personnel to "routine, repetitive tasks" the completion of which was essential for various government functions.[299]

Since then, the increase in the number of bureaucracies may have moderated but the persistence of bureaucracies in U.S. governance (and in the private sector) has not.[300] Max Weber would ascribe this persistence of bureaucracy to its efficiency; as I noted earlier,[301] he believed that the "decisive reason for the advance of bureaucratic organization has always been its purely technical superiority over any other form of organization."[302] Indeed, at one point Weber noted that the "fully developed bureaucratic mechanism compares with other organizations exactly as does the machine with the non-mechanical modes of production."[303]

Many of us, I suspect, might take issue with Weber's views about the inevitable efficiency of bureaucracies, if only because of our own experiences in dealing with them. In § IV(B), I will do something similar, i.e., I will analyze the relative efficacy with which the bureaucracies we examined in § III are, or are likely to be, capable of dealing with cyber-threats. My analysis of this issue will be based on the premise that Weber's views on the inherent efficiency and consequent superiority of bureaucratic organization were, in critical respects, the product of the world in which he lived. I develop that premise in the remainder of this section.

---

resulted in the creation of agencies to monitor the administration and implementation of those grants. *See id.* at 91-93.

[299]James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 81. As others have noted, bureaucracies "excel[] at routine, standard tasks". James R. Holmes & Janne E. Nolan, *Render unto Caesar: Bureaucracy and Nonproliferation after the Iraq War?,* 28-WTF Fletcher Forum of World Affairs 73, 79 (2004). *See also* Carroll Seron, *The Impact of Court Organization on Litigation,* 24 Law & Soc'y Rev. 451, 459 n. 18 (1990) ("a necessary precondition for bureaucratization is the routinization of tasks").

[300]One author attributes this, at least in part, to the development of "self-perpetuating agencies", i.e., to the creation of agencies that produce "a set of political relationships that make exceptionally difficult further alteration of that program". James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 93. Wilson also notes that Georg Simmel believed that organizations tend "to acquire the characteristics" of the institutions "with which they are in conflict, so that as government becomes more bureaucratic, private organizations" will tend to "become bureaucratic as well." *Id.* at 80.

[301]*See supra* note 1 & accompanying text.

[302]From Max Weber: Essays in Sociology 214 (trans. & ed. by H. Gerth & C. Mills 1958). *See also* Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 337 (bureaucracy is the "most rational known means of carrying out imperative control over human beings").

[303]From Max Weber: Essays in Sociology, *supra* note 302 at 214.

Weber was born before the German Empire became a unified state, which occurred when he was six years old.[304] In the next forty years, the Empire went through a period of rapid industrialization and population growth.[305] Weber consequently matured in a country that was establishing itself as a modern nation-state and a modern industrial power.[306] He, in fact, became "a champion of German industrialization."[307]

It is therefore not surprising that Weber's work emphasizes the shift from an older, essentially ad hoc social order based on traditional, status-based authority to a system based on "rational" authority, i.e., on "a belief in the `legality' of . . . rules and the right of those elevated to authority under such rules to issue commands".[308] Rational authority was coming to dominate the systems around him: the newly-established German state and the corporate entities that were the architects of the industrialism.[309] It is also not surprising that Weber viewed this new type of authority, and the bureaucracies which it created and sustained, as vastly superior to the older systems that had gone before.[310]

Given all this, it is only reasonable to infer that the validity of Weber's views as to the inherent operational superiority of the bureaucratic form of organization depends on

---

[304]*See id.* 3-8. *See also* "German Empire," Wikipedia, http://en.wikipedia.org/wiki/German_Empire.

[305]*See, e.g.,* "German Empire," *supra* note 304. *See also* From Max Weber: Essays in Sociology, *supra* note 302 at 49.

[306]*See id.* (noting that Germany had "the most powerful army in the world" and soon had a navy that "was second only" to that of the British Empire).

[307]Fritz Ringer, Max Weber: An Intellectual Biography 2 (2004).

[308]Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 328. Weber identified several essential characteristics of the rational-legal, bureaucratic organization: the "organization of official functions bound by rules"; a "specified sphere of competence" for the bureaucracy itself and for each unit within the bureaucracy; the "organization of offices follows the principle of hierarchy, that is, each lower office is under the control and supervision of a higher one"; "specialized training" and "acts, decisions, and rules" that are "formulated and recorded in writing. *See id*. at 330-332.

[309]*See* Fritz Ringer, Max Weber, *supra* note 307 at 64-65, 220-221. *See also* Jurgen Kocka, Industrial Culture and Bourgeois Society: Business, Labor, and Bureaucracy in Modern Germany, 1800-1918 130, 148 156-157, 198-204 (1999). *See, e.g.,* From Max Weber: Essays in Sociology, *supra* note 302 at 232 ("Everywhere the modern state is undergoing bureaucratization").

[310]Weber recognized that forms of bureaucratic organization had existed for centuries. *See, e.g.,* From Max Weber: Essays in Sociology, *supra* note 302 at 204-224 (e.g., ancient Egypt, Rome, China). He noted that these early bureaucracies differed from the organizations emerging in the nineteenth century in various ways, the most important of which was that the latter were based on rational-legal authority. *See id.* at 204-228.

the context in which the bureaucracy operates.[311] His views emerged in an era when each society, each nation-state, was a closed system, i.e., was subject to the constraints noted in our analysis of the bifurcated approach states use to control threats to internal and external order.[312] Weber consequently assumed a territorially-defined nation-state, the stable boundaries and sovereign authority of which circumscribed the functioning of the bureaucracies that carried out various essential functions, including those charged with maintaining order.[313]

This meant that the state could respectively assign discrete bureaucracies a "specified sphere of competence,"[314] i.e., turf, which was exclusive to that organization, and rely on each bureaucracy to formulate and enforce the rules necessary to carry out the functions assigned to it.[315] The system was predicated on a multi-faceted division of labor among agencies, with each being the sole arbiter of its sphere of responsibility.[316] This system therefore encompassed the bureaucracies that were respectively assigned responsibility for ensuring internal and external order, along with those that were given other functions. Our concern, of course, is only with the bureaucracies that are charged with maintaining order.

In § II, we saw that our use of cyberspace erodes the territorial integrity of nation-states and, in so doing, creates new and difficult challenges for the organizations that are given this responsibility. The issue we now need to address is whether bureaucracy continues to be a viable organizational model insofar as the tasks of maintaining internal and external order are concerned or whether it is an institution that has, at least to some extent, outlived its utility in this regard. We take up that issue in the next section.

B. The Fallacy of Inevitability

The tendency of a principle to expand itself to the limit of its logic. . . .[317]

---

[311]In other words, it is reasonable to assume there will be a direct relationship between the extent to which the context is empirically and doctrinally isomorphic to the context in which Weber developed his views on bureaucracy and the extent to which bureaucracy functions at the level of efficiency Weber attributed to it.

[312]*See supra* § II. *See also* Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 156 (modern nation-state is based on an "administrative and legal order" that "claims binding authority, not only over the members of the state" but also "over all action taking place in the area of its jurisdiction). Weber notes that the state is "thus a compulsory association with a territorial basis." *Id.*

[313]*See supra* note 312.

[314]Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 330.

[315]*See supra* note 308. *See also supra* note 5.

[316]*See supra* note 5.

[317]Benjamin N. Cardozo, The Nature of the Judicial Process 51 (1921).

As we saw in the section above, bureaucracy, like all social institutions, is a tool: a way of organizing human activity to achieve particular results. It has no inherent validity, no inevitable superiority over other ways of organizing human endeavor. It is the pragmatic product of an ad hoc evolutionary process.[318]

And as I noted earlier, bureaucracy organizes human activity hierarchically, into a descending series of offices, each of which is "under the control and supervision of a higher" office.[319] Bureaucracy's reliance on hierarchically ordered positions comes from the military, which adopted hierarchical organization several millennia ago.[320] Like the military, modern bureaucracy is based on a tiered organizational structure in which tasks of are allocated in order of their decreasing importance to the increasingly less important positions in the bureaucracy.[321] And because authority is allocated in a similar fashion, the functionaries in an organization carry out their duties subject to the supervision and

---

[318]*See, e.g.,* Peter Berger & Thomas Luckmann, The Social Construction of Reality, *supra* note 291 at 54-55:

> It is impossible to understand an institution . . . without an understanding of the historical process in which it was produced. Institutions . . . control human conduct by setting up predefined patterns of conduct, which channel it in one direction as against the many other directions that would theoretically be possible.

See also id. at 60:

> An institutional world . . . is experienced as an objective reality. It has a history that antedates the individual's birth. . . . It was there before he was born, and it will be there after his death. This history itself, as the tradition of the existing institutions, has the character of objectivity.

[319]Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 331. *See supra* note 308.

[320] *See, e.g.,* John Arquilla & David Ronfeldt, Swarming & the Future of Conflict 13 (2005). *See also* From Max Weber: Essays in Sociology, *supra* note 302 at 221-224. For non-military uses of bureaucratic organization in the ancient world, *see id.* at 204 (e.g., ancient Egypt, Rome and China).

The military developed hierarchical organization to meet its new goal of "achiev[ing] advantages in mass" over an adversary. *See* John Arquilla & David Ronfeldt, Swarming & the Future of Conflict, *supra* at 13. Hierarchies let commanders create and utilize "well-articulated formations" of troops. *See id*. Hierarchically organized armies therefore replaced the melee, which was the earlier, "chaotic form of war". *Id.* at 10.

[321]*See supra* note 308. *See also* From Max Weber: Essays in Sociology, *supra* note 302 at 197 ("The principles of office hierarchy and levels of graded authority mean a firmly ordered system of super- and subordination in which" lower offices are supervised by higher ones).

approval of the functionaries above them.[322] As Weber approvingly noted, modern bureaucracy has many of the characteristics of a well-functioning machine.[323]

Machines, as we all know, are well-suited for specific, repetitive tasks but have no ability to adapt to changing circumstances -- to innovate.[324] That characteristic, which bureaucracies clearly share with machines, has not been particularly problematic for them in the decades since Weber lauded bureaucracy's inherent supremacy over other types of organization.[325]

It has not been problematic, I submit, because this semi-mechanical, segmented organizational structure is well suited for carrying out the routine, repetitive tasks societies have for the most part assigned to bureaucracy over the last century.[326] Or, I should say, the bureaucratic organizational structure is in the abstract well-suited for this purpose; as a matter of historical reality, its efficacy in this regard has been eroded by various circumstances over the last few decades, at least in the United States.[327] Some of this erosion can be attributed to structural and/or operational flaws in the bureaucratic model of organization; others are the product of changing conditions in the environment in which bureaucracies now operate.[328]

The challenges emerging from cyberspace are an example of the latter and exacerbate the former, at least as far as bureaucracies charged with maintaining order are concerned. Given this, one might expect the United States to be experimenting with new approaches to maintaining internal and external order, at least with regard to threat activity originating in cyberspace. That, though, is not the case: As we saw in § III, the federal government's efforts to improve the country's cyber-threat-control structure are all predicated on bureaucratic solutions. So unless we assume the federal government

---

[322]*See supra* note 321.

[323]*See supra* note 303 & accompanying text.

[324]If, for example, the electricity goes out, my refrigerator shuts down; it does not have the ability to find and utilize an alternative power source. And if my coffee-maker quits working, my toaster will not be able to fill in for it.

[325]*See, e.g.,* note 289 & accompanying text, *supra.*

[326]*See supra* note 299 & accompanying text.

[327]*See, e.g.,* note 5, *supra.*

[328]As to the former, *see supra* note 5. In the United States, bureaucracy seems to have become a victim of its own success; proliferating and expanding bureaucracies create the turf wars described earlier. *See supra* note 5. And the United States' approach to bureaucracy has increasingly displayed the tendency noted above, i.e., a propensity to over-use and over-orchestrate this concededly useful form of organization. I will return to this issue later in the text above.

is descending into madness,[329] there must be some rational explanation for this ostensibly illogical behavior.

There is a rational explanation for the government's persistent reliance on bureaucracy as the strategy used to address challenges, even when it is apparent that the challenges involve circumstances that make the use of bureaucratic solutions highly problematic. I ascribe it to what I call the fallacy of inevitability (or, business as usual): the tendency to assume that reified, institutionalized patterns of behavior are necessary and, indeed, inevitable.[330] If a person, or an organization, assumes that institutionalized methodologies are inevitable, i.e., are a "given," the person/organization will not attempt to develop new methodologies in order to deal with new challenges. I do not mean to suggest that our hypothetical person/organization makes a conscious choice to eschew innovation; rather, institutions establish "`how these things are done'"[331] and, in so doing, implicitly foreclose consideration of alternatives.[332]

I believe the fallacy of inevitability explains the behaviors we reviewed in § III. To understand why I believe that, we need to review the behaviors in question according to the institution -- i.e., military, law enforcement and private sector -- to which they pertain.

1. The Military

We will begin, as we did in § III, with the military. As we saw above, the federal government initially intended to improve the military's ability to respond to cyber-threats by creating a new threat-specific bureaucracy, i.e., a cyberspace command, which would have become part of the Air Force.[333] That approach would have centralized the U.S. military's cyberspace operations in a single bureaucratic organization – Air Force Cyber Command – which might, or might not, have been a good thing.

This initial approach, like all the approaches we examined in § III(A), was predicated on the classic, Weberian tactic of creating a dedicated bureaucracy to take responsibility for a specific function. It would have made a cadre of Air Force cyber-specialists responsible for controlling cyber-threats (at least, those that fall within the military's sphere of responsibility), [334] and thereby avoided the segmented response

---

[329]"`Insanity: Doing the same thing over and over again and expecting different results.' Albert Einstein." Albert Einstein – Quotes, http://www.alberteinsteinsite.com/quotes/einsteinquotes.html.

[330]*See supra* note 296 & accompanying text. *See also supra* notes 291 & 318.
[331]Peter Berger & Thomas Luckmann, The Social Construction of Reality, *supra* note 291 at 59.

[332]*See id.* at 53 (institutionalization of behaviors narrows choices and, in so doing, frees us from "the burden of `all those decisions'").

[333]*See supra* § III(A)(1).

[334]*See supra* § II.

authority that, among other things, is an integral part of U.S. law enforcement.[335] In other words, the initial approach would have assigned cyberspace response authority to the Air Force, just as the federal government long ago assigned maritime response authority to the Navy and aerial response authority to the Air Force. Since the parsing of kinetic threat response authority for those combat domains has worked reasonably well, employing a similar strategy for cyberspace response authority might have been a good approach if bureaucratic response processes were effective with regard to cyber-threats. As we saw in §§ II and III, they are not.

The government's initial approach to assigning cyberspace response authority also suffered from another defect: Unlike air space and maritime space, cyberspace is not a "space."[336] Cyberspace is a global communication system of tremendous, and continually evolving, complexity and sophistication.[337] It is consequently impossible to segregate the myriad of activities that create and sustain cyberspace from the real-space actors and assets with which they interact.[338] It would, therefore, have been difficult for the Air Force Cyber Command that was the focus of the initial approach to

---

[335]*See supra* § III(B). *See also supra* note 4.

[336]*See, e.g.,* Blumenthal v. Drudge, 992 F. Supp. 44, 48 n. 7 (D.D.C. 1998):

> `[C]yberspace is not a `space'. . . . At least not in the way we understand space. It's not located anywhere; it has no boundaries; you can't `go' there. At the bottom, the Internet is really more idea than entity. It is an agreement we have made to hook our computers together and communicate by way of binary impulses and digitized signals. . . .

[337]*See, e.g.,* Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 139 (April 12, 2001 – as Amended through October 31, 2009), http://jitc.fhu.disa.mil/jitc_dri/pdfs/jp1_02.pdf (defining cyberspace as a "global domain . . . consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers").

[338]Each of the five branches of the U.S. military uses cyberspace in its various activities. *See, e.g.,* "NIPRNet," Wikipedia, http://en.wikipedia.org/wiki/NIPRNet (non-secure network used by the U.S. military to exchange unclassified information and to access the Internet); DISN Data Services, http://www.disa.mil/services/data.html (NIPRNet). *See also* Command, Control, Communications, Computers and Information Technology (C4IT) Service Center, U.S. Coast Guard (July 21, 2011), http://www.uscg.mil/c4itsc/; Annual Cyber Awareness Training, U.S. Marines (February 27, 2011), http://www.marines.mil/news/messages/Pages/MARADMIN118-11.aspx; Gerry J. Gilmore, *Navy Moves to Meet Information Age Challenges,* U.S. Navy (October 2, 2009), http://www.navy.mil/search/display.asp?story_id=48723; Karl Weisel, *Cyber Hawks Help Keep Network Safe,* U.S. Army (August 13, 2008), http://www.army.mil/article/11631/; U.S. Air Force, Careers, http://www.airforce.com/careers/#s_computer. *See generally* Jon P. Jurich, *Cyberwar and Customary International Law,* 9 Chi. J. Int'l L. 275, 278 (2008) (Department of Defense "uses over two million computers and more than ten thousand local area networks, most of which are linked to . . . the larger internet").

implement that responsibility.[339] Instead of simply fighting "in" cyberspace, the proposed Air Force Cyber Command would have been dealing with threats that were vectored through its own computer systems plus the systems operated by the Army, the Navy, the Marines and the Coast Guard, as well as with systems owned and operated by civilians and civilian entities.[340] There would therefore have been no distinct spatial domain as to which that U.S. Air Force Cyber Command would have had exclusive response authority.

Why did the federal government abandon its initial, Air Force Cyber Command-predicated approach to controlling cyberthreats? My research suggests there are two, not-necessarily incompatible explanations.

One is that the government decided that various factors, including those noted above, made it impossible to follow the until-then business as usual approach by treating cyberspace as merely another spatially-demarcated war-fighting domain and allocating domain-specific response authority to a single branch of the military. It therefore elected to employ a generic version of the business as usual approach by assigning cyber-threat response authority to a unified command, i.e., to a command that incorporates forces from the various branches of the U.S. military.[341]

---

[339] *See supra* § III(A).

[340] *See note* 338, *supra. See, e.g.,* David M. Hollis, *USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command,* NDU Press JFQ 48 (Issue 48, 3d Quarter 2010), http://www.ndu.edu/press/lib/images/jfq-58/JFQ58_48-53_Hollis.pdf:

> [M]ilitary operations in the cyberspace domain are radically different from military operations in the other warfighting domains. . . .[C]yberspace is an artificial construct and does not primarily exist in the natural world, while the other domains exist in nature. Cyberwar/NETWAR will primarily be fought over network terrain that is owned and operated by private sector entities, many of them multinational corporations. Military operations in the cyberspace domain simultaneously include physical and logical maneuver space.

[341] *See supra* notes 145 - 146 & accompanying text (unified command). By a generic version of the business as usual approach, I mean that the government decided to treat cyber-threat control as a function assigned exclusively to the military. *See supra* § II.

While it is can be difficult to identify the motivations behind national security decisions, I find support for the proposition that this is, in fact, why the government abandoned its cyberspace-as-exclusive-Air-Force-domain approach to cyber-threat control. *See, e.g.,* Robert Gates, Secretary of Defense, Memorandum: Establishment of a Subordinae Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations 1 (June 23, 2009), http://online.wsj.com/public/resources/documents/OSD05914.pdf ("Department of Defense requires a command that . . . remains focused on the integration of cyberspace operations"). *See also* David M. Hollis, *USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command, supra* ("Because of the unique nature of the domain, no one Service is responsible for operations to protect national cyberspace (unlike the other domains)"). Colonel Hollis argued that because cyberspace is not a

As a result, the Air Force's Cyber Command and the cyber commands the other branches had established were folded into Cyber Command, which, as we saw above, is a "subunit of U.S. the Strategic Command."[342] And as we also saw above, despite this presumptive integration the branch cyber commands continue to develop and field their respective, idiosyncratic cyberspace capabilities.[343]

That brings us to the other explanation for why the government abandoned the initial, Air Force Cyber Command-based approach: It capitulated to the fallacy of inevitability by allowing each of the five branches of the U.S. military to develop its own cyber command under the aegis of the U.S. Strategic Command's Cyber Com.[344] The capitulation was apparently a victory of turf over logic and pragmatism, a concession to the continuation of business as usual.[345]

---

physical domain, cyber-threat response authority must be unified in one entity. *See id.* For U.S. Strategic Command, *see supra* notes & accompanying text.

Hollis argued that since creating a unified combatant command is a lengthy, time-consuming process, one that in this instance faces "internal DOD opposition", the Defense Department should adopt the initial, interim step of creating a "subunified command". *See id.* at 48-49. He maintained that this would "unify and streamline . . . military cyberspace capabilities" and avoid a scenario in which "each individual Service develop[ed] and field[ed] an uncoordinated and disjointed set of cyberspace capabilities." *See id.* at 51. And while Hollis was writing after the decision had been made to create Cyber Command, he pointed out that the then-current

> U.S. Government efforts to conduct cyberdefense/cyberwar/NETWAR are badly fragmented and require . . . integration/synchronization of overall cyberspace operations. Resources to defend . . . the cyberspace domain are woefully inadequate, and many of the resources are acquired and deployed in an unfocused and uncoordinated fashion.

Id. at 53.

[342]William Jackson, *DOD Creates Cyber Command as U.S. Strategic Command Subunit,* Federal Computer Week (June 24, 2009), http://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx?Page=1. *See supra* § III(A)(1).

[343]*See supra* note 341. *See also* § III(A).

[344]*See supra* § III(A).

[345]*See, e.g.,* Peter A. Buxbaum, *US: Cyberwar Turf Battle Continues,* ISN (August 28, 2008), http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch-Archive/Detail/?id=90624&lng=en (Air Force's creating its Cyber Command "provoke[ed] a turf war" with other branches of the military); *Inside the Cyber Command Turf Battle,* Defense Tech (August 15, 2008), http://defensetech.org/2008/08/15/inside-the-cyber-command-turf-battle/ (noting the Pentagon's possible plan to "kill" Air Force Cyber Command and implying that the other branches, plus various civilian agencies, were competing for the funds to be spent on cyber security). A 2011 article attributed the

The result, as we saw earlier, is that we now have six cyber-threat response bureaucracies, one for each of the five branches of the military plus Cyber Command, which is to weave the branch-specific commands together into a coherent, effective response effort.[346] As I write this, Cyber Command has been in existence for over a year but has yet to establish policies and procedures that can integrate the branch commands into a unified operational cyber-command.[347] I, for one, am skeptical both as to Cyber Command's ability to achieve such an integration and as to its ability to protect citizens of the United States from the cyber-threats for which is has, or will have, responsibility.

My skepticism as to the first issue is the product of Cyber Command's current lack of progress in this area and of the fact that the branch cyber commands seem to be pursuing their own agendas.[348] My skepticism as to the second issue is the product of a circumstance noted earlier, i.e., that since the "markers" traditionally used to distinguish between crime/terrorism and war are of little utility in cyberspace, it is likely to be difficult, if not impossible, for the military to reliably determine the nature of an attack quickly enough to allow them to launch a timely response.[349]

In other words, my skepticism is the product of the limitations of bureaucracy. Cyber Command exists because the government decided that the best approach to cyber-threat control was to create not one bureaucracy (the original Air Force Cyber Command) but a series of bureaucracies, all but one of which is a sub-bureaucracy operating within an already existing bureaucracy. Cyber Command is a free-standing bureaucracy which is, in effect, charged with taking at least partial control of the sub-bureaucracies away from the respective military bureaucracies to which each belongs. In other words, Cyber Command's mission is essentially to create its own bureaucratic

---

capitulation to turf battles among the various branches of the military. *See Cyber War: Pentagon Takes on Cyber Enemies, Other Agencies,* Defense Industry Daily (August 16, 2011), http://www.defenseindustrydaily.com/cyberwar-department-defense-doctrine-response-06931/ (Air Force "made an early grab" to be the dominant branch in cyberspace but faced "fierce opposition from both the Army and the Navy"). As to bureaucracies inherent tendency to battle over turf, *see supra* note 5.

I also find inferential support for this assumption in the branches' continuing efforts to develop their own, idiosyncratic cyber-operations plans. *See, e.g., LandWarNet 2011: U.S. Army Detail Cyber Vision 2020,* Shephard News (August 24, 2011), http://www.shephard.co.uk/news/digital-battlespace/landwarnet-2011-us-army-detail-cyber-vision-2020/9814/; Amber Corrin, *Navy's Cyber Unit Scans Horizon for New Challenges,* Defense Systems (June 21, 2011), http://defensesystems.com/articles/2011/06/08/cyber-defense-navy-cyber-programs.aspx.

[346]*See supra* § III(A).

[347]*See supra* § III(A).

[348]*See supra* § III(A). *See also supra* note 345.

[349]*See supra* § III(A). I return to this issue later in this section.

turf out of turf appropriated from each of the five branches. It is difficult to imagine how it can succeed.[350]

My skepticism is also the product of another of the limitations of bureaucracy, at least when it utilized in the context of cyber-threat control. As we saw above, the United States' threat-control structure is bifurcated, with law enforcement responding to crime and terrorism (internal threats) and the military responding to warfare (external threat). As we also saw, this bifurcation has produced a massive series of (i) federal, state and local law enforcement bureaucracies and (ii) military bureaucracies. The bifurcation, and the bureaucracies it produced and on which its operations are predicated, assumes that it is possible to assign a "specified sphere of competence" to each bureaucracy. That means, as we saw earlier, that (i) the military responds only to warfare and (i) federal, state and local law enforcement responds only to crime or terrorism. This allocation of response authority, as we saw above, assumes it is possible for law enforcement and the military to be able to parse threats according to the relevant sphere of competence into which they fall. In other words, it assumes military and law enforcement officials can quickly ascertain whether a threat falls within their sphere of competence. Since the use of cyberthreats undermines, if it does not eradicate, the reliability of the factors on which each relies in making this determination, it undermines their ability to determine when a threat falls within their area of responsibility.[351]

Essentially, the U.S. military now has a highly-articulated, stove-piped[352] system of response authority which is, to say the least, exceedingly problematic when it comes to controlling cyberthreats. Even if we assume, for the purposes of analysis, that Cyber Command and/or its subordinate cyber commands will be able to ascertain which cyber-attacks are military in nature and which are not, they are still unlikely to be able to respond with the speed and efficacy required to establish a viable cyber-threat control system. Like guerrilla warfare, cyber-attacks are asymmetric, i.e., they do not conform to the model of conflict in which adversaries with reasonably equal forces simultaneously engage in combat.[353] Cyber-attacks can be directed at diverse targets and can occur over a more or less extended period of time; it can, therefore, be functionally impossible for those charged with controlling such attacks to launch a reciprocal response before

---

[350]*See supra* note 5.

[351]*See supra* § II.

[352]*See supra* note 5.

[353]*See, e.g.,* Reshaping the Military for Asymmetric Warfare, Center for Defense Information (October 5, 2001), http://www.cdi.org/terrorism/asymmetric.cfm. *See also* Robert Vamosi, *Guerrilla Cyber Warfare: Are We Thinking Defensively,* Security Week (September 1, 2011), http://www.securityweek.com/guerilla-cyber-warfare-are-we-thinking-defensively. *See generally* Chico Harlan & Ellen Nakashima, *Suspected North Korean Cyberattack on Bank Raises Fears for S. Korea, Allies,* Washington Post (August 29, 2011), http://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html.

the initial attack has ended.[354] It can also, as we saw in §II, be impossible for those who are charged with cyber-threat control to identify who was responsible for such attacks, in order to retaliate at a later point in time.[355]

Given all that, it is almost certain that criminals, terrorists and/or hostile nation-state cyber commands will be able to exploit the huge, elaborately segmented network of bureaucracies described above to their advantage. Bureaucracies tend to move slowly; indeed, I suspect that as a general matter, the speed with which a bureaucracy moves is in inverse proportion to the size and complexity of the bureaucracy.[356] If I am correct, that does not augur well for the cyber-response effort outlined above. Aside from anything else, it may mean that while Cyber Command and/or one or more of its constituent commands is/are attempting to ascertain the nature and source of an attack, the attack can proceed to completion, after which the attackers fade into the anonymous world of cyberspace.

In the next section, we will consider the extent to which the fallacy of inevitability affects U.S. law enforcement's ability to respond to cyber-attacks.

2. Law Enforcement

As we saw earlier, the bureaucratization of U.S. law enforcement is to a great extent the product of strictures imposed by our federal system of government:[357] Law enforcement agencies are divided into two primary categories – federal and state – and the latter is respectively subdivided into state and local agencies.[358] As we also saw, in terms of the number of agencies and the number of officers, federal law enforcement is much smaller than state law enforcement, taken as a whole.[359]

This disparity in the number and size of state and federal law enforcement agencies is attributable to the fact that for most of the United States' history, crime "was seen as a uniquely local concern and the power to prosecute rested almost exclusively

---

[354]*See, e.g.,* Christopher Williams, *Stuxnet: Cyber Attack on Iran "Was Carried Out by Western Powers and Israel,"* The Telegraph (January 21, 2011), http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html.

[355]*See, e.g.,* Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia,* New York Times (May 29, 2007), http://www.nytimes.com/2007/05/29/technology/29estonia.html.

[356]In other words, the larger and more complex the bureaucracy, the slower it responds.

[357]*See supra* § III(B)(2). *See also supra* note 4.

[358]*See supra* § III(B)(2). *See also supra* note 4.

[359]*See supra* note 4.

in the states".[360] That began to change in the "last third of the nineteenth century", as Congress increasingly used its Commerce Clause power to criminalize conduct that had been prosecutable only at the state level.[361] This trend accelerated in the twentieth century, in large part because automobiles made it much easier for perpetrators to flee across state lines, thereby frustrating pursuit by state officers.[362] Notwithstanding that, the default responsibility for criminal law enforcement remains with the states, which is why there is such a difference in the relative size and staffing of state and federal law enforcement agencies.

As we also saw above, U.S. law enforcement, unlike the military and private sector entities, has so far not been the target of legislative and/or other efforts designed to enhance the nation's ability to control cyber-threats.[363] As things currently stand, then, the current law enforcement bureaucracy bears the responsibility to control the incidence of cyber-threats that fall within its "sphere of competence,"[364] i.e., crime and terrorism.[365] It is therefore useful to review the evolution of that bureaucracy, which is for the most part a legacy: the product of two essentially independent factors.

One is, as we saw earlier, that U.S. law enforcement agencies operate within a prescribed geographical area: [366] They all operate within the territory of the United States; the United States' ability to enforce its criminal law ends, for the most part, at its borders.[367] Federal law enforcement agencies' geographical jurisdiction is essentially co-extensive with the United States' territorial jurisdiction. [368] State and local agencies operate within the territory of the state that created them; state agencies' geographical jurisdiction is co-extensive with the state's territory, while local agencies' geographical

---

[360]American Bar Association Task Force on the Federalization of Criminal Law, The Federalization of Criminal Law 6 (1999), http://www.nacdl.org/public.nsf/legislation/overfederalization/$FILE/fedcrimlaw2.pdf.

[361]*See id.*

[362]*See, e.g.,* Kathleen F. Brickey, *Criminal Mischief: The Federalization of American Criminal Law,* 46 Hastings L.J. 1135, 1142-1144 (1995).

[363]*See supra* § III(B)(2).

[364]*See supra* note 308.

[365]*See supra* § II.

[366]*See supra* § III(B)(2).

[367]*See, e.g.,* Charles Doyle, Extraterritorial Application of American Criminal Law 1, Congressional Research Service (2010), http://www.fas.org/sgp/crs/misc/94-166.pdf. *See also id.* at 12-20.

[368]*See supra* § III(B)(2). As we saw in § III(B)(2), federal law enforcement agencies' authorized sphere of investigation is further circumscribed by substantive jurisdictional requirements.

jurisdiction will be limited to the county, municipality or other subdivision of the state that employs them.[369] Each federal, state or local agency is a bureaucracy because all U.S. law enforcement agencies were organized, or re-organized, according to the principles Weber outlined in his work on bureaucracy.[370]

The result – a complex, segmented but often overlapping series of law enforcement bureaucracies – is a well-established phenomenon, the product of the partitioned jurisdictional response authority dictated by the United States' distinctive federal system.[371] It is also a relatively new phenomenon: The bureaucratization of U.S. law enforcement began in the mid-nineteenth century, as American cities adopted the new, hierarchically-organized, quasi-military policing model Robert Peel had established in England.[372] Until then, American law enforcement was informal, predicated "on the medieval institutions of the constable, the night watch, and the hue and cry -- institutions that `drew no clear lines between public and private.'"[373]

Peel's model became the dominant model of policing in the United States, which brings us to the second factor: Peel's reliance on a quasi-military model as the basis for his police forces. Like members of the military, law enforcement officers wear uniforms and operate within hierarchically-structured organizations that rely on military ranks and a chain of command.[374] Law enforcement's reliance on a semi-military bureaucratic structure is quite reasonable, since their mission, like that of the military, involves conflict and the use of physical force in a real-space context. The respective missions of law enforcement and the military and the contexts in which they respectively operate are therefore consistent with the assumptions Weber made in heralding the efficiency of the

---

[369]*See supra* § III(B)(2). *See also supra* note 4.

[370]*See, e.g.,* David J. Bordua & Albert J. Reiss, Jr., *Command, Control, and Charisma: Reflections on Police Bureaucracy*, 72 American J. Sociology 68 (1966). *See also* Daniel C. Stiles, *Border Crisis: Time for A New Collective Review of Tri-Nation Border Security,* 29 Transp. L.J. 299, 307 (2002); Mark Tushnet & Jennifer Jaff, *Critical Legal Studies and Criminal Procedure,* 35 Cath. U. L. Rev. 361, 381 (1986).

[371]*See supra* § III(B)(2).

[372]*See, e.g.,* David A. Sklansky, *The Private Police*, 46 UCLA L. Rev. 1165, 1202-1209 (1999).

[373]*Id.* at 1205. *See also id.* at 1206:

> [S]erving as constable or watchman was . . . an unpaid civic obligation, but in practice everyone who could afford to hire a substitute did so. . . . Those with sufficient resources hired additional protection, and the boundary between private guards and public watchmen often was indistinct.

(notes omitted).

[374]*See, e.g., id. See also* David J. Bordua & Albert J. Reiss, Jr., *Command, Control, and Charisma: Reflections on Police Bureaucracy, supra* note 370.

bureaucratic model of organization.[375] This means that bureaucracy is a suitable organizational model when both operate in real-space.[376]

But law enforcement, like the military, must now operate in cyberspace as well as in real-space. And cyberspace creates new challenges for law enforcement, just as it does for the U.S. military.[377] The challenges cyberspace creates for law enforcement are the converse of General Alexander's problem,[378] i.e., law enforcement agencies now have to deal with attacks from abroad which can be war and/or crime and/or terrorism.[379]

As I explain elsewhere, the traditional threats – crime, terrorism and war – can morph in cyberspace, so what appears to be a cybercrime is actually cyberwarfare or cyberterrorism or a hybrid, e.g., cyberwar/crime.[380] As I have also explained, cyberspace

---

[375]*See supra* § IV(A).

[376]*See supra* §§ II & IV(A).

[377]*See supra* § III(A).

[378]*See supra* § III(A).

[379]*See, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 20.

[380]*See id.* The incident I use to illustrate the phenomenon of morphing in cyberspace and the legal conundrums it creates occurred in 2001: Gary Lauck, a U.S. citizen who lives in Nebraska, was operating websites that distributed pro-Nazi material; distributing such material in Germany is a crime. *See, e.g.,* Susan W. Brenner, *Mixing Metaphors,* CYB3RCRIM3 (April 22, 2009), http://cyb3rcrim3.blogspot.com/2009/04/mixing-metaphors.html. Since the material was accessible in Germany, German authorities concluded that Lauck was violating German law, i.e., was committing a crime. After unsuccessfully trying to have Lauck extradited to Germany to face charges for the sites' content, German Interior Minister Otto Schily suggested Germany use Distributed Denial of Service to overwhelm the sites with signals and effectively shut them down. *See id.*

Germany never launched such attacks, but assume, for the purposes of analysis, that it had: What type of cyber-attack would have resulted? On the one hand, a nation-state (Germany) would have attacked property in territory of another nation-state (the U.S.), a scenario that is to some extent analogous to Japan's attack on Pearl Harbor. *See id.* But unlike the Pearl Harbor attack, Germany's hypothesized cyber-attack would have been directed at civilian, rather than military, targets, which to some extent undermines the premise that it would have been an act of cyberwarfare. *See id.* That premise is supported, however, by the fact that Germany's hypothesized cyberattack would have violated the territorial integrity of the United States, i.e., would have struck at the heart of the U.S. sovereignty. *See id.* One can, then, argue that the hypothesized attack that did not happen would have constituted cyberwarfare. *See id.*

But one can also argue that if the hypothesized attack had happened, it would have constituted cybercrime, since it was directed at property belonging to a particular civilian, was not intended to impact on a larger civilian audience and was in no way intended to

eliminates the barriers that historically made warfare the exclusive province of nation-states; it is therefore not only possible but likely that non-nation-state actors will launch cyberattacks that are intended to undermine the sovereign viability of a nation-state, i.e., attacks that are indistinguishable from warfare.[381]

U.S. law enforcement agencies have traditionally been responsible for controlling crime and terrorism.[382] They are neither authorized to, nor capable of, responding to acts of war, including cyberwar.[383] And aside from anything else, it would not be prudent for the United States to alter this state of affairs and authorize its law enforcement officers to respond to cyberattacks without regard to whether the attack appears to be cybercrime, cyberterrorism or cyberwarfare. This could, among other things, allow hostile state (or hostile non-nation-state) actors to "game" the system: They launch what appears to be an act of cyberwarfare by Nation-State X on a target in Illinois in an effort to tempt local law enforcement officers to respond with offensive digital force directed at Nation-State X. If the Illinois officers responded, and if Nation-State X was, in fact, not responsible for the Illinois attack, it would mean the United States had launched an unprovoked cyber-

---

actually undermine the sovereignty of the United States. *See id.* This argument is further supported by the fact that the United States, along with a number of other countries, makes the launching of a Distributed Denial of Service attack a crime. *See id.* Such an attack is treated as a crime if it is launched by a civilian and is directed either at a civilian target or at a government agency. *See id.* So if the United States had chosen to approach the hypothesized cyber-attack as an attack launched by Schily as a civilian on a civilian target, then the U.S. could have charged him with cybercrime and asked the German authorities to extradite him for prosecution in the United States. *See id.*

[381]*See* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 20. *See also US Standards Body Issues Warning to Energy Suppliers over Cyber Attacks,* InfoSecurity (August 8, 2011), http://www.infosecurity-magazine.com/view/19930/us-standards-body-issues-warning-to-energy-suppliers-over-cyber-attacks/. *See, e.g.,* Mark Landler & John Markoff, *Digital Fears Emerge After Data Siege in Estonia, supra* note 355.

[382]*See supra* § II. That changed, to some extent, in the aftermath of the 9/11 attacks. *See, e.g.,* Thomas J. Bogar, *Unlawful Combatant or Innocent Civilian? A Call to Change the Current Means for Determining Status of Prisoners in the Global War on Terror*, 21 Fla. J. Int'l L. 29, 68 (2009):

> Before 9/11, terrorism was considered a law enforcement issue, and terrorists as criminals. Since then, terrorism abroad is considered a military matter and terrorists as enemy combatants to be detained as such or prosecuted before military commissions.

(notes omitted). The post-9/11 shift in how extraterritorial terrorists are treated may be to some extent a harbinger of the changes that will occur in how nation-states treat transnational cybercriminals.

[383]*See supra* § II.

attack on an innocent state. If Nation-State X were to respond in kind, the incident could escalate into a real cyberwar between the two countries.[384]

The United States and other nation-states therefore confront both a problem and a dilemma: The problem, as we saw in § II, is that the ease with which cyber-attacks transcend national borders and ever-eroding utility of the "markers" countries have relied on to differentiate between internal and external threats to order make the bifurcated approach to threat-control increasingly problematic.

The military is charged with responding to attacks from hostile nation-states, i.e., attacks from abroad, but it can be difficult and time-consuming to determine whether a cyberattack (i) is from abroad or is a domestically-based attack that has been routed through foreign servers to disguise its true nature and/or (ii) is crime, terrorism or warfare. This impedes the military's ability to respond with the speed, discrimination and efficacy needed to deter attacks from hostile nation-states.[385] Law enforcement is charged with responding to domestic attacks carried out by civilians, i.e., crime and terrorism, but it can be difficult, resource-intensive and time-consuming to determine if a cyberattack is (i) is domestic or originated from abroad and (ii) is crime, terrorism or warfare.[386] Their respective problems interact to create uncertainty as to whether a particular cyberattack falls within law enforcement's or the military's "sphere of competence."[387]

Logically, this creates the possibility that in a given instance both, or neither, will respond. If neither responds, the attacker(s) successfully targeted the United States, inflicted some quantum of damage on its civilians and/or assets and thereby to eroded the country's ability to maintain internal or external order.[388] If both respond, this could

---

[384]Scenarios such as this are far from implausible, as states like China "harness[] the potential" of their "hacktivist communit[ies] for executing military operations . . . across the Web." Dancho Danchev, *China's Blue Army: When Nations Harness Hacktivists for Information Warfare,* ZDNet (May 31, 2011), http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare/8686.

[385]*See supra* § III(A)(2).

[386]*See supra* § II. *See, e.g.,* U.S. Department of Justice, Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law (May 20, 2011), http://www.justice.gov/criminal/pr/testimony/2011/crm-testimony-110510.html ("Investigating . . . multi-actor, multi-national crimes is extremely resource intensive").

[387]*See supra* note 308.

[388]While an isolated failure to respond is unlikely to seriously challenge the United States' ability to maintain order, a repeated series of failures will do so. *See, e.g.,* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime,* 23 J. Marshall J. Computer & Info. L. 659, 691 (2005) (utility of sanctions in deterring criminal conduct is a function of the perceived risk of being caught). *See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues,* 5 U. Pitt. J. Tech. L. & Pol'y 2, (2005). *See also* Margaret Raymond, *Penumbral Crimes,* 39 Am. Crim. L. Rev. 1395, 1404 (2002); Harold G. Grasmick & Robert J. Bursik, Jr., *Conscience, Significant*

result in an unintended escalation of the situation, e.g., if a cybercriminal attacks a U.S. bank and becomes the target of retaliative action by U.S. law enforcement and the U.S. military, the latter's involvement could escalate the incident to cyberwarfare.[389]

That brings us to the dilemma noted above: How can we resolve the problems outlined above? The obvious, pragmatic answer is that we should somehow combine the military and law enforcement, at least insofar as cyber-attacks are concerned. As things currently stand, the Posse Comitatus Act of 1878 prohibits the U.S. military from "performing a domestic civilian law enforcement function."[390] The Posse Comitatus Act is one of the bulwarks of the bifurcated approach to threat-control we examined in § II, but it is merely the product of legislative action; we could t repeal the Act, thereby eliminating the statutory provision that bars the integration of civilian and military personnel. Since no correlate provision bars U.S. law enforcement from assisting the U.S. military,[391] we should then be able to develop an integrated, law enforcement-military cyber-threat response system, which would presumably resolve the problems outlined above.

While that strategy has an undeniable logic, I, for one, do not believe it is the appropriate way to approach the problems noted above. For one thing, it contravenes the "deeply held American principle that civilian and military spheres should be kept distinctly separate", a sentiment to which the nation's founders clearly subscribed.[392] One could argue that the concerns responsible for Posse Comitatus and the founders' desire to segregate civilian and military threat control functions apply with less urgency when conduct migrates from real-space into cyberspace,[393] but I do not find that a convincing argument. Aside from anything else, we have already learned that what happens in cyberspace can, and does, impact on our lives in real-space so, to employ another cliché, I see this as a slippery slope, which I, at least, would prefer to avoid.

I also have another, far more pragmatic, objection to the possibility of fusing law enforcement's and the military's respective efforts to control cyberthreats: I fear the impact the fallacy of inevitability would have on such a step. Absent a dramatic and

---

Others, and Rational Choice: Extending the Deterrence Model, 24 Law & Soc'y Rev. 837, 841 (1990).

[389]*See supra* note 380.

[390]Mark David "Max" Maxwell, *The Enduring Vitality of the Posse Comitatus Act of 1878,* 37 Prosecutor 34 (May/June 2003). *See* 18 U.S. Code § 1385.

[391]*See, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 22 at 444-455.

[392]Scott R. Tkacz, *In Katrina's Wake: Rethinking the Military's Role in Domestic Emergencies,* 15 Wm. & Mary Bill Rts. J. 301, 307 (2006). *See also* William C. Banks, *Normalization of Homeland Security After 9/11: The Role of the Military in Counterterrorism Preparedness and Response,* 64 La. L. Rev. 735, 740, 741 (2004); Nathan Canestro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus,* 12 Wash. U. J. L. & Pol'y 99, 99 (2003).

[393]*See, e.g.,* Susan W. Brenner, *Cyber Threats, supra* note 8 at 294.

quite unanticipated change in our approach to these matters, it is almost certain that if we embarked on such an effort it would result in our creating yet another bureaucracy: a cyber-military-law enforcement agency.[394] That would only exacerbate the problems we examined earlier, i.e., we would have a massive, highly segmented (real-space only) military bureaucracy, a massive, highly segmented (real-space only) law enforcement bureaucracy and a no-doubt massive, no-doubt highly segmented (cyberspace only) military-law enforcement bureaucracy. This approach would merely compound the problems we examined earlier and would suffer from yet another defect: It does not incorporate the participation of civilians, which, as I noted earlier, will be essential in developing an effective cyber-threat control structure.[395]

In § V, I argue that we need to develop a fluid, flexible, networked approach for dealing with cyberthreats. In the next section, I explain why civilians are an essential part of such an effort.

3. Civilians

As we saw in § II, the bifurcated approach to threat-control assumes threats are readily divisible into "inside" (crime/terrorism) and "outside" (warfare). We also saw that this is not a viable assumption when threats are vectored through cyberspace.[396] As things currently stand, the "markers" we once used to differentiate between private threats (crime/terrorism) and sovereign threats (war) are of little, if any, utility when it comes to cyberspace. Individuals can accomplish what was once the sole province of nation-states, and nation-states can use state actors or civilian nominees to carry out what appear to be cybercrimes and/or cyberterrorism but are in reality attacks designed to advance a sovereign's covert agenda, i.e., cyberwarfare.[397] The result, to paraphrase Yeats, is that things threaten to fall apart and anarchy seems a viable prospect.[398]

I emphasize this to illustrate that what was once unthinkable has become a very real possibility: Civilians, who became noncombatants under the modern law of armed conflict,[399] are now on the front line of cyber conflict. Civilians have for years been the targets of cybercrime;[400] civilian entities may have been, and most certainly will be, the

---

[394]We might, as I note elsewhere, refer to it as the Cyber Security Agency. *See id.*

[395]*See* § IV, *supra.*

[396]*See supra* § II.

[397]*See supra* note 384 & accompanying text.

[398]*See* William Butler Yeats, The Second Coming (1919), http://www.potw.org/archive/potw351.html.

[399]*See, e.g.*, J. Ricou Heaton, *Civilians at War: Reexamining the Status of Civilians Accompanying the Armed Forces,* 57 A.F.L. Rev. 155, 157-163 (2005).

[400]*See, e.g.,* Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace 9-38 (2010).

targets of cyberterrorism and cyberwarfare.[401] This means that at least some civilians will have to participate in cyber-conflict,[402]a reality the legislative proposals we examined in § III(C)(1) all acknowledge.

The respective drafters of those proposals and I consequently agree on the need for civilian participation but part company on how that participation is to be incorporated into a cyber-threat control structure. My goal in this section is to explain how, and why, the approach the proposals we examined in § III(C)(1) take to this task is flawed in ways that will erode the efficacy of the cyber-threat response efforts they respectively outline.

As I noted in § III(C)(1), the two Senate proposals and the White House proposal are all lengthy and complex, in part because each deals with a variety of issues, some of which are not directly related to integrating civilians into a cybersecurity effort.[403] In this section, we will focus only on the provisions of the proposals that deal with this particular issue. And we will not parse those provisions in detail. Instead, I will explain why the general approach these proposals take to this task is flawed – yet another product of the fallacy of inevitability.[404]

All of the proposals put the Department of Homeland Security (or, more precisely, a sub-bureaucracy of the Department) in charge of ensuring that private entities involved in the operation of the nation's critical infrastructure will establish and then implement (i) security measures designed to improve their ability to avoid or withstand cyber-attacks and (ii) plans for responding to cyber-attacks.[405] The entities will be required to comply with these requirements as long as their company is deemed to be part of the nation's

---

[401]*See, e.g.,* Richard A. Clarke & Robert Knake, Cyber War: The Next Threat to National Security and What to Do about It xi ("The most likely targets [of cyberwarfare] are civilian in nature") (2010). *See also id.* (it is . . . the civilian population of the United States and the publicly-owned corporations that run our key national systems that are likely to suffer in a cyber war). *See also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* note 22 at 426-427, 454-455.

[402]I use the generic term cyber-conflict because, as we saw above, it will be difficult to parse attacks into cybercrime, cyberterrorism and/p cyber-warfare*. See supra* § II(C).

[403]The White House proposal, for example, includes provisions creating new federal cybercrimes and modifying provisions of existing federal cybercrime law. *See* White House Cybersecurity Proposal: Law Enforcement Provisions Related to Computer Security, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security.pdf. It also includes provisions governing data breach notification. *See* White House Cybersecurity Proposal: Data Breach Notification, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf.

[404]*See supra* § IV(B).

[405]*See supra* notes 227 & 228 & accompanying text. As I noted earlier, the precise nature of the latter, i.e., of the plans for responding to cyber-attacks is not specified. *See supra* note 264 & accompanying text.

critical infrastructure.[406] And as we saw in § III(C)(1), the proposals all establish a new, Department of Homeland Security-based bureaucracy to implement these and the other requirements they impose on those entities.

The White House and Senate proposals are therefore products of the fallacy of inevitability, i.e., they all create a new bureaucracy that is charged with enforcing the obligations to create and implement the measures noted above.[407] As I explained earlier, this approach is, as a general matter, flawed when it is utilized in an effort to address cyberthreats.[408] I believe it is also flawed in a very specific respect when it is applied to incorporating civilian participation into a cybersecurity effort; the specific flaw is a product of the particular context in which the approach is implemented.

In order to explain why I believe that, I need to digress briefly to outline a modest taxonomy of bureaucracies. For the purposes of this analysis, I will divide bureaucracies into two types: implementary bureaucracies and regulatory bureaucracies.

Implementary bureaucracies are directly charged with carrying out certain tasks, traditionally in real-space.[409] Military organizations and law enforcement agencies are examples of implementary bureaucracies; the hierarchical division of authority and labor that is a defining characteristic of bureaucracy facilitates their ability to carry out their respective tasks in the physical world.[410] The same is true of businesses, educational institutions, government agencies charged with carrying out other specific tasks (e.g., FEMA) and similar entities.[411]

Implementary bureaucracies are first-tier bureaucracies, that is, they are directly responsible for carrying out functions that are useful, if not essential, to the survival of a particular society. The specific functions for which an implementary bureaucracy is responsible act as an imperative that focuses its efforts on, and shapes its organization for, the efficient, effective implementation of the tasks necessary for carrying out those

---

[406]*See, e.g.,* Cybersecurity and Internet Freedom Act of 2011, *supra* note 233 at § 254(c)(3).

[407]As we saw earlier, a sphere of competence and the creation and enforcement of rational-legal rules are essential characteristics of Weberian bureaucracies. *See supra* note 308.

[408]*See, e.g.,* § IV(A), *supra.*

[409]*See, e.g.,* James Q. Wilson, What Government Agencies Do and Why They Do It, *supra* note 5 at 25 (noting that bureaucracies are charged with carrying out certain "critical tasks").

[410]*See, e.g.,* § IV(A), *supra.*

[411]*See, e.g.,* Stephen M. Bainbridge, *Participatory Management within a Theory of the Firm,* 21 J. Corp. l. 657, (1996) (noting that "Henry Ford and others designed firms as highly centralized, hierarchical bureaucracies"). *See also* Federal Emergency Management Agency, Wikipedia, http://en.wikipedia.org/wiki/Federal_Emergency_Management_Agency.

functions.[412] When Weber approvingly described bureaucracies as machines, he was referring to implementary bureaucracy.[413]

Regulatory bureaucracies, on the other hand, are second-tier bureaucracies: They are charged not with directly implementing the useful or essential functions noted above but with "regulating" how implementary bureaucracies carry out those functions.[414]

---

[412]This, in turn, reduces the likelihood of mission creep, in which a bureaucracy loses focus on the areas for which it was originally given responsibility and "seek[s] to expand" its authority, and activities, into other areas. *See, e.g.,* Peter B. Rutledge, *Medillin, Delegation and Conflicts (of Law),* 17 Geo. Mason. L. Rev. 191, 206 (2009). As this author notes, a "precisely defined mandate reduces the opportunity" for a bureaucracy to lose focus and begin to dissipate its efforts on tasks for which it was not originally responsible. *See id.* at 206 n. 74. And as others have noted, bureaucratic turf battles can also result in mission creep. *See, e.g.,* Matthew Bobby, *DOD-DHS Memorandum of Understanding Aims to Improve Cybersecurity Collaboration,* Harvard National Security Journal (November 15, 2010), http://harvardnsj.com/2010/11/dod-dhs-memorandum-of-understanding-aims-to-improve-cybersecurity-collaboration/. *See generally supra* note 5.

[413]*See supra* note 323 & accompanying text. I base this assertion primarily on the fact that in his work on bureaucracy and other issues, Weber relied on "ideal types," rather than on particular empirical phenomena. *See, e.g.,* Talcott Parsons, *Introduction*, Max Weber, The Theory of Social and Economic Organization, *supra* note 1 at 12-13. As Parsons explains, the

> ideal type as Weber used it is both abstract and general. It does not describe a concrete course of action, but a normatively ideal course. . . . It does not describe an individual course of action, but a `typical' one – it is a generalized rubric within which an indefinite number of particular cases may be classified.

Id. at 13. As Parsons also noted, a Weberian ideal type "involve[s] a fixed relation between the values of the various variable elements involved", which means that "it is limited in certain respects." *Id.* My contention is that when Weber wrote about the inherent, machine-like efficiency of bureaucracies, he was referring to an ideal type bureaucracy that in many, if not most, respects conformed to the model of implementary bureaucracy described above. *See supra* notes 319 - 323 & accompanying text.

I also base this assertion the fact that the "other" type of bureaucracy – the regulatory bureaucracy discussed later in the text above – only began to emerge in the last two decades of the nineteenth century, and was therefore not well entrenched at the time Weber wrote admiringly of the "efficiency" of bureaucracies. *See, e.g.,* James Q. Wilson, *The Rise of the Bureaucratic State, supra* note 95 at 94-98 (emergence of regulatory bureaucracy in the United States). *See also supra* notes 304 - 307 & accompanying text.

[414]*See, e.g.,* Ontario Public Appointments Secretariat, http://www.pas.gov.on.ca/scripts/en/generalinfo.asp#1:

> Regulatory agencies make independent decisions (including inspections, investigations, prosecutions, certifications, licensing, rate-setting, etc.)

The Federal Aviation Administration, for example, "regulate[s] and oversee[s] all aspects of civil aviation" in the United States.[415] And the Federal Communications Commission "regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories."[416]

As part of regulating the activities of implementary bureaucracies, regulatory bureaucracies establish -- and enforce -- standards and other rules that govern the performance of the first-tier bureaucracies.[417] The regulatory bureaucracies' charge is to ensure that the implementary agencies subject to their jurisdiction carry out the tasks assigned to them in a safe, effective manner.[418] Regulatory bureaucracies therefore add an extra "sphere of competence" and an extra layer of rules and rule-implementation to the implementary bureaucratic structure Weber admired for its efficiency.[419]

The Department of Homeland Security-based bureaucracy that would be created by the proposals we examined in § II(C)(1) would be an unusual entity. On the one hand, it would appear to be a regulatory bureaucracy: Unlike the military and law enforcement bureaucracies we examined above,[420] it would not be directly charged with protecting the

---

> which limit or promote the conduct, practice, obligations, rights, responsibilities, etc. of an individual, business or corporate body. . . .

The description given above applies with equal validity to regulatory bureaucracies because regulatory agencies are synonymous with regulatory bureaucracies. Regulatory agencies are not, however, synonymous with bureaucracies, as such. As noted above, Implementary bureaucracies differ in critical respects form regulatory agencies. *See supra* notes 409 - 411 & accompanying text.

[415]"Federal Aviation Administration," Wikipedia, http://en.wikipedia.org/wiki/Federal_Aviation_Administration. *See also* Regulations & Policies, Federal Aviation Administration, http://www.faa.gov/regulations_policies/.

[416]What We Do, Federal Communications Commission, http://www.fcc.gov/what-we-do.

[417]*See, e.g.,* FCC Rulemaking, Federal Communications Commission, http://www.fcc.gov/rulemaking. *See also supra* note 414.

[418]*See, e.g.,* Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors,* 103 Colum. L. Rev. 749, 757 n. 30 (2003) (regulatory bureaucracies begin with "`policy formation' -- a `process whereby the agency interprets and translates legislative goals into rules, standards, and plans of action'" and then proceed to enforce "`these agency directives,' including the `operating routines used by field-level personnel and applied to targets of regulation, decisions about the application of regulations, and means for obtaining compliance with rules'") (quoting Keith Hawkins & John M. Thomas, *The Enforcement Process in Regulatory Bureaucracies*, in Keith Hawkins & John M. Thomas, Enforcing Regulation 3, 10 (1984)).

[419]*See supra* notes 308 - 310 & accompanying text.

[420]*See supra* §§ II(A) & III(A)-(B),

United States and its citizens from threats originating here and/or abroad. Instead, the proposed Department of Homeland Security bureaucracy would, like the regulatory bureaucracies noted above, act as an intermediary between the government and the civilian implementary bureaucracies which carry out various tasks that are useful and/or essential for the country's survival and/or prosperity.[421]

Unlike a regulatory bureaucracy, however, this new Department of Homeland Security-based bureaucracy would not be charged with ensuring that the entities it oversees carry out the civilian tasks assigned to them in a safe, effective manner. It would instead be charged with imposing, and enforcing, an obligation to assume an additional, unrelated task: a measure of responsibility for protecting the country from cyber-threats. As we saw in § III(C)(1), this entity would be responsible for identifying the private sector entities that would be subject to this new responsibility, for working with each entity to develop the security measures and response plans noted above and for monitoring, and ensuring, the continuing efficacy and implementation of both.[422]

So while this agency is at least implicitly styled as a regulatory bureaucracy, it is in fact something quite different: It is essentially the twenty-first century version of impressment.[423] The proposed Department of Homeland Security agency (i) would not be responsible for monitoring how the entities subject to its authority carry out their purely civilian functions (unless, of course, that impacts on cyber-threat control) (ii) but would be responsible for imposing a new non-civilian function, or set of functions, on these entities.[424] That has a number of implications, one of which is that the civilian entities which become the focus of this bureaucracy's efforts are likely to resist, since they are being drafted into a military-law enforcement effort of uncertain scope and possibly unlimited duration.[425] The authors of the Senate proposals clearly recognized that entities are likely to resist being conscripted into this effort, because they included a

---

[421]The White House and Senate proposals all include provisions concerning law enforcement and the military's involvement in cyber-threat control activity, but they will not be discussed here because the focus of this discussion is on involving civilians in this activity. *See supra* § III(C)(1).

[422]*See supra* note 405 & accompanying text. *See also supra* § III(C)(1).

[423]*See, e.g.,* Casey B. Mulligan & Andrei Shleifer, *Conscription as Regulation,* 7 Am. L. & Econ. Rev. 85, 88 (2004) (describing impressment as "the forced recruitment of individuals with little or no compensation or regulation of service terms or length"). For more on this, *see* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts,* 43 Vand. J. Transnat'l L. 1011 (2010); Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties,* 13 SMU Sci. & Tech. L. Rev. 249 (2010).

[424]For some thoughts as to how this might be structured, *see* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1056-1062.

[425]Unlike traditional military conscripts, their status would not shift entirely from civilian to member of the U.S. military. *See id.* It is more likely that they would devote much of their time at work to performing their usual, civilian functions, and only be "called up" to carry out the quasi-military/law enforcement functions on occasion. *See id. See also* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties, supra* note 423.

provision in their second bill that lets companies file a suit appealing their designation as a critical infrastructure component subject to the efforts of this new Department of Homeland Security bureaucracy. [426]

I see at least three significant flaws in the approach the Senators and the White House are taking to the task of enhancing the United States' ability to control cyber-threats.[427] The first is that their strategy relies on a pseudo-regulatory bureaucracy to bring civilian entities into this effort instead of trying to incorporate them into what is really needed, i.e., an implementary bureaucracy that departs in certain ways from the conventional implementary bureaucracies on which we currently rely. We will return to this issue in § V.

The second flaw is that the approach proposed by the Senators and the White House simply recycles bureaucracy as the way to improve the United States' ability to control cyberthreats. It implicitly, and incorrectly, assumes that the strategy nation-states rely on to control real-space threats can be effective in controlling cyberthreats.[428] As we saw in § II, while this strategy has been effective in controlling territorially-based threats, it is not an effective approach to controlling cyberthreats.

That brings us to the third flaw: Because it is predicated on a the efforts of a quasi-regulatory bureaucracy, the strategy proposed by the Senators and the White House takes a prescriptive approach to achieving certain conduct, i.e., implementing cybersecurity measures and response plans. As we saw earlier, the bureaucratic model of organization allocates authority in diminishing increments to a hierarchically structured set of "offices", each of which has a specialized function.[429] Bureaucracies are therefore predicated on a top-down strategy in which the "offices" with greater authority adopt and enforce rules that impose certain requirements (i) on offices within that organization that have lesser authority or (ii) on external entities that are subject to the organization's supervision.[430] As we saw in § II, this model has worked well in the military and in other organizations charged with achieving concrete objectives in real-space. It is unlikely to

---

[426]*See, e.g.,* Cybersecurity and Internet Freedom Act of 2011, *supra* note 233 at § 254(c)(2) (company file an appeal "seeking judicial review" of the entity's "final agency action" in the U.S. District Court for the District of Columbia).

[427]As I noted above, other members of Congress have submitted their own cybersecurity legislative proposals. *See supra* note 238. Since those proposals are similar in at least certain respects to the White House and Senate proposals, we will not examine them separately.

[428]*See supra* § II.

[429]*See supra* note 308.

[430]*See supra* note 308. In other words, Weberian bureaucracies rely on prescriptive rules, i.e., rules that prescribe certain behaviors and/or results and impose sanctions for failing to comply with what is required. For more on prescriptive rules, *see* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime,* 23 J. Marshall J. Computer & Info. L. 659, 690-691 (2005).

work well in incorporating civilians and civilian entities into an effective cyber-threat control effort, for several reasons.

For one thing, the bureaucracy created by the Senators' and the White House's proposals would not be a free-standing bureaucracy with its own mission, discipline and *esprit de corps.*[431] The proposed Department of Homeland Security-based bureaucracy would be an essentially parasitic entity that would intrude into, interfere with and alter the otherwise routine operations of the civilian entities that were subject to its authority. The measures this Department of Homeland Security-based bureaucracy imposed on these entities would alter their routine functioning and mission in various ways and would, as a result, almost certainly generate resistance.[432]That means these measures, like any prescriptive rules,[433] would have to be enforced, which can be an onerous task for any bureaucracy. Given the highly complex, constantly evolving nature of the cybersecurity measures this agency would be imposing and the number of civilian entities and civilians involved in their implementation, effective enforcement would be an incredibly complex, challenging and expensive undertaking.[434]

It would almost certainly be ineffective. In § II, we saw that the approach nation-states have traditionally taken to controlling real-space threats (crime, terrorism and warfare) becomes increasingly ineffective as threats are vectored through cyberspace. That discussion focused primarily on how cyberspace's erosion of the significance of territory undermines the efficacy of this system by blurring the distinction between "inside" (crime/terrorism) and "outside" threats (warfare). In so doing, it implicitly demonstrated how cyberspace erodes the efficacy of the hierarchical model of organization.

As I explained elsewhere, technology eliminates the need,

> and indeed the ability, to focus on localized activity. Communication technologies . . . free us from spatial constraints; we can communicate with anyone anywhere in the world. New technologies generate new types of social organization, and communication technologies have created the network. Networks tend to displace hierarchies because hierarchical organization evolved to deal with real-world activity; as such,

---

[431]Weber emphasized the role discipline played in the effectiveness of military bureaucracy. *See* From Max Weber: Essays in Sociology, *supra* note 289 at 153, 261. *See also* Talcott Parsons, The Structure of Social Action 507 (2d ed. 1968) ("Above all, bureaucracy involves discipline").

[432]For more on this, *see, e.g.,* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 1058-1060.

[433]*See supra* note 430.

[434]For the difficulties involved in enforcing a much simpler set of cybersecurity rules, *see* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 90-95.

> it is not an effective means of organizing technologically-mediated activities.[435]

Networks are lateral, fluid systems. Social networks – the informal associations of individuals that arise in cyberspace – usually have no fixed structure, constituency or endurance.[436] They are often opportunistic, i.e., they emerge for a more or less specific reason and dissipate when that imperative declines or disappears.[437] Social networks of whatever size and constituency have proven quite effective in evading law enforcement and military bureaucracies.[438] Their success in this regard is, as we saw in § II, in large part attributable to the irrelevance of territory in cyberspace, but is also a function of the fact that cyberspace decentralizes power.

As we saw in § II, the threat control model sovereigns have employed for millennia is predicated on the assumption that the use and/or threatened use of the sovereign's power, i.e., physical force, will keep threats at an acceptable level. This assumption incorporates a subsidiary assumption: that the sovereign will be able to use or credibly threaten to use its power against actual or potential criminals, terrorists or hostile states. As we saw in §§ II and III, sovereigns have long relied on hierarchically organized groups (e.g., armies, law enforcement agencies) to impose or to threaten to impose their power on actual or potential criminals, terrorists or hostile states. As we saw in § III, the Senators' and the White House's cybersecurity proposals attempt to do essentially the same thing in cyberspace.

The problem, as we saw in §II, is that there is no fixed, identifiable target: It can be difficult if not impossible to ascertain (i) who is responsible for an attack, (ii) whether he/she is a criminal, terrorist or state/non-state warrior, (iii) where he/she is/was was when the attack was launched and (iv) whether launching a responsive cyber attack would violate United States law, international law and/or the law of another nation-state. A bureaucracy charged with making these determinations (and, if appropriate, launching a retaliatory attack) would find the task time-consuming at best and impossible at the worst.[439] The difficulties inherent in this task are exacerbated by several factors, one of which is that the postulated bureaucracy will not confront only one enemy, only one attack, at a time. The Pentagon, for example, is attacked thousands of times every

---

[435]Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime, supra* note 430 at 668 (notes omitted). For the link between hierarchical organization and real-world activity, *see* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 78.

[436]*See, e.g.,* "Anonymous," Wikipedia, http://en.wikipedia.org/wiki/Anonymous_(group)/

[437]*See, e.g., id.*

[438]*See, e.g., id.*

[439]*See* § II, *supra.*

day,[440] and it is only one target. The bureaucracy outlined in the Senators' and the White House's cybersecurity proposals would be charged with protecting not only the United States' military and other government systems from online attacks, but also what appears to be a substantial segment of the private sector.[441] That *might* be a viable scenario if the attacks fell into a single, simultaneous and relatively homogenous category, i.e., online versions of the 1941 attack on Pearl Harbor. As we saw in § II, that will not be true; online attacks vary in (apparent) place of origin, nature, duration, objective and a number of other factors.[442] They can also evolve very quickly, which would make the proposed bureaucracy's task even more difficult.

That difficulty would be further exacerbated by the Department of Homeland Security-based bureaucracy's need to coordinate its determinations and responses with those of Cyber Command and, presumably, law enforcement.[443] Neither the need for, nor a method of implementing, such coordination is included in any of the proposals; they include provisions that allow information to be shared across these sectors, but none of the proposals addresses how the military, law enforcement and private sector participants would coordinate their efforts in the face of cyberattacks.[444] Absent such coordination, they are, at best, likely to duplicate their respective efforts and, at worst, to interfere with those efforts.[445]

I could note other problems with the proposals we examined in § III but I believe (or at least I hope) I have made my point: The proposals are an exercise in futility (as well as a concession to the fallacy of inevitability) because they assume a hierarchically ordered exercise of concentrated sovereign authority can be an effective threat control

---

[440]*See, e.g.,* David Martin, *First Look Inside the Military's Cyber War Room,* CBS News (July 14, 2011), http://www.cbsnews.com/stories/2011/07/14/eveningnews/main20079585.shtml.

[441]*See*, e.g., Cybersecurity and Internet Freedom Act of 2011, *supra* note 233 at § 101(a).

[442]*See supra* § II.

[443]As we saw in § III, neither of these is a unitary entity: Cyber Command encompasses the five subordinate cyber commands and U.S. law enforcement encompasses agencies at the federal, state and local levels. *See supra* § III and note 4. There would, therefore, have to be reciprocal coordination among all of these agencies and the proposed Department of Homeland Security-based bureaucracy we examined in § III(C).

[444]*See* Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act, *supra* note 236 at § 7(e); Cybersecurity and Internet Freedom Act of 2011, *supra* note 233 at § 242.

[445]If we continue to rely on the fallacy of inevitability, we could address this state of affairs by creating an *uber*-cyber-threat-control bureaucracy and charging it with monitoring and coordinating the respective efforts of these sectors. That, of course, would only compound the problems noted above.

mechanism in a non-spatial context in which such exercises are meaningless. In the next section I outline an alternative approach, one that has its own challenges.

V. . . . and Beyond?

My primary purpose in writing this article is to explain why our persistent reliance on Weberian bureaucracies as the engines of our threat-control processes is not only problematic, but is increasingly counter-productive. I have for years argued that a top-down approach to cybersecurity is ultimately futile and that we therefore need to develop an approach that is compatible with the realities of virtual-space.[446]

It is, of course, much easier to criticize an existing system than to outline a viable alternative. This is particularly true given that, as we saw earlier, we are socialized to assume the inevitability of the institutions that surround us.[447] Those institutions and the embedded routines and assumptions that maintain them are so deeply ingrained in the fabric of our lives that it is exceedingly difficult to imagine a radically different approach to governing or educating ourselves . . . or protecting ourselves. As I wrote this article, I tried to recall an instance in history in which the citizens of a society realized that the viability of one of the institutions on which they relied was in an irreversible decline and rationally set about implementing an alternative. Since I am not intimately familiar with the occurrences in all societies throughout all the preceding millennia, I cannot state this as a certainty, but it is my reasonably confident belief that this has not happened. What happens in practice is that the institution (and, in some instances, the society it supports) fails (Roman Empire) or is destroyed by civil unrest (French Revolution).

If that is true, then this article may be an exercise in futility. I, however, choose to believe that even if none of our predecessors were prescient enough to replace a failing institution with a viable alternative, this does not mean deliberate institutional innovation is not possible. I believe it is possible; whether it will be practicable for the United States to replace the legacy threat-control system on which it currently relies is another matter. I suspect that whether the United States succeeds in this regard depends to a great extent on whether, and when, we realize we have a problem. As I outlined the current state of cyber-threat-control in this country and the proposals that have been put forward to improve its efficacy, I was tempted to cite the *Emperor's New Clothes*;[448] I cannot understand why knowledgeable people in government and in the private sector do not point out the obvious futility of the measures being proposed. I assume they either find that politically problematic or realize it would accomplish nothing.

That brings me back to the task at hand: How do we structure and implement a threat-control structure that can be effective enough against cyber-threats to maintain the baseline of order we, as a society, require in order to survive and prosper? As I explained in detail earlier, I do not believe such an approach can be based on a top-

---

[446] *See, e.g.,* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 105-106.

[447] *See supra* § IV(A).

[448] "Emperor's New Clothes," Wikipedia, http://en.wikipedia.org/wiki/The_Emperor's_New_Clothes.

down, hierarchically organized system. The networked communication system that creates and sustains what we experience as cyberspace is essentially an instrumental and experiential overlay that subsumes the empirical reality in which we exist. As such, it eludes the territorially-based governance systems that have maintained order for centuries; cyberspace is more analogous to the environment that existed before those systems evolved, i.e., to the state of affairs that prevailed in Britain after the Roman Empire fell.

The fall of the Roman Empire left Britain with no formal institutional structures to ensure order. Because human societies cannot survive without the ability to maintain a baseline of order, and because central governance was lacking, the citizens of that time and space developed their own, "networked" approach to maintaining order. Essentially, all of the adult, able-bodied males in a community were in charge of fending off external threats and controlling internal threats.[449] The colonists brought this system with them to the United States, where it survived into the nineteenth century, when it was replaced by the formal institutions we rely on today.[450]

The community-based threat-control structure that evolved, and proved very effective, in post-Roman Britain was predicated on an attitude we do not share: The citizens of post-Roman Britain realized they were responsible for protecting themselves in real-space because no one else could. We do not share that attitude because we are the products of a system in which civilians are passive, i.e., have no responsibility to protect themselves or their nation-state (unless they are conscripted into the military).[451] We expect the government to protect us; we do not see ourselves as having any responsibility for threat-control in the real or virtual worlds.

That attitude is not problematic with regard to real-space threats. As we saw in § II, our military and law enforcement officers are quite capable of maintaining the baseline of order required in the physical world. There is therefore no need for us to assume any responsibility for this task, and several reasons why we should not.[452]

---

[449]For a more detailed account of the origins and operation of this system, *see, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 8 at 165-175; Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts, supra* note 28 at 174-175; Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 61-63. *See also* David A. Sklansky, *The Private Police,* 46 UCLA L. Rev. 1165, 1195-1198 (1999). If a qualified male member of the community failed to participate in this system, he was subject to punishment. *See, e.g.,* J. Michael Olivero, Cyril D. Robinson & Richard Scaglion, Police in Contradiction: The Evolution of the Police Function in Society 20 (1994).

[450]*See, e.g.,* Susan W. Brenner, Cyber Threats, *supra* note 8 at 165-175; Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 61-63. *See also supra* § II.

[451]See*, e.g.,* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/terrorism/warfare, supra* 20 at 445-446.

[452]Since order-control in the physical world entails the use of physical force, it is not advisable to encourage, or tolerate, civilian participation in this endeavor. Given the potentially dangerous nature of the activity involved and often sophisticated techniques

As we have seen, it is becoming increasingly apparent that our military and law enforcement officers cannot adequately protect us from cyber-threats. As noted above, the Senators' and the White House's cybersecurity proposals recognize that an effective cyber-threat control structure requires the participation of civilians. They recognize this but, in my humble opinion, their approach to implementing this participation errs in two regards: It assumes civilian participation is limited to private sector entities that are part of the nation's critical infrastructure; and it assumes that to be effective such participation must be imposed and enforced by an external government bureaucracy.

The flaw in the first assumption is that it is based on the erroneous proposition that cyberthreats, like crimes and acts or terrorism and acts of war, have an identifiable dynamic and an ascertainable goal. By identifiable dynamic, I mean cyber-attacks are inferentially likely to be directed at high-value targets, just as banks are more likely to be robbed than churches, terrorists are more likely to attack civilian spaces than police stations and bombers are more likely to attack destroyers than farms. And by having an ascertainable goal, I mean cyber-attacks are inferentially designed to achieve certain ends, just as crimes are usually intended to enrich the perpetrator, acts of terrorism are intended to intimidate a civilian population and acts of war are intended to undermine the viability of an opposing nation-state. The proposals we examined above incorporate this proposition because they are an attempt to combat known threats. Because of that, they ignore the fact that in cyberspace, vulnerabilities are not confined to overtly high-value targets; an unsecured system in a small business could be used to launch a cascading attack that could take down a large financial institution (or a series of such institutions). Because almost everything in cyberspace is, or can be, linked to almost everything else in cyberspace, any unsecured computer and/or any unreliable or alienated employee can become the source of an attack. To be effective, a cyber-threat control structure needs to be as all-encompassing as possible; it should replicate the community-based approach post-Roman Britains took to controlling the real-space threats they confronted.

We explored the flaw in the second assumption in §IV. As we saw there, relying on a mandate enforced by an external government bureaucracy is, aside from anything else, almost certain to generate some resistance from the civilians who are subject to its dictates.

Logically, an effective cyber-threat control structure must be catholic in scope and participation must be voluntary.[453] That brings us back to the issue I noted earlier:[454]

---

utilized by law enforcement and the military, it is prudent to exclude civilians from this undertaking.

[453]That does not mean we could not impose sanctions on those who contumaciously refused to participate. There is precedent for such a step. *See supra* note 449. And as I argue elsewhere, enforcing an obligation to participate in a general cyber-threat control effort is neither inconsistent with obligations we otherwise impose on citizens nor should it be particularly onerous to enforce. *See, e.g.,* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security, supra* note 8 at 105-107. *See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues,* 5 U. Pitt. J. Tech. L. & Pol'y 2, 50-88 (2005).

[454]*See supra* notes 281

To implement such a structure, the government must overcome its citizens' disinclination to become involved in any type of security effort. But overcoming the disinclination is a delicate, difficult matter for the leaders of the United States or, for that matter, of any country: They would have to convince the populace that the government cannot protect them from cyber-threats while, at the same time, maintaining civilian confidence in the government's ability to protect them from other threats.[455]

More precisely, they would have to convince the citizens of the United States (or any other country) that the government *alone* cannot protect them from cyber-threats but can still protect them from real-space threats. The goal would be to couple reassurance (stability in the physical world) with a limited admission of vulnerability (chaos in the virtual world) and to use the latter to recruit civilians into a cyber-threat-defense effort.[456] The United States actually did something similar in the late 1940s and early 1950s. In an attempt to prepare citizens for a nuclear attack, the Department of Defense and a several universities developed an initiative that was designed to reduce Americans' "terror" of nuclear weapons by recruiting them into a civil defense effort that would be part of the overall national security effort.[457]

---

[455]One article describes the prevailing corporate attitude as follows:

> `What are the subconscious assumptions that companies bring to the issue of foreign cyber-attacks on their networks?,' a senior Senate staffer who works on cyber-issues asked. . . . `They assume that if something bad happens government will take care of the losses. They act like they don't really believe that a bank could get completely taken out, or that a tech giant could get its whole lunch eaten. . . .'

Michael Joseph Gross, *Enter the Cyber-Dragon, supra* 244 at 12. I suspect we will see the disinclination eroded gradually, as news outlets and other media publicize leaked information about cyberattacks and, in so doing, begin to cultivate attitudes similar to those that have driven many citizens to invest in alarm systems and burglar bars.

[456]It is unclear, at this point, whether the civilian participation contemplated by the Senators' and the White House's proposals would encompass offensive measures, as well as purely defensive measures. *See generally supra* notes 264 & 269.

[457]*See, e.g.,* Guy Oakes, The Imaginary War: Civil Defense and Cold War Culture 33-77 (1994). As this author notes, this initiative was based on the premise that the

> problem of protecting the United States from nuclear attack could be solved, but only by transforming American life through the construction of `a permanent civil defense system.' Because the national security crisis was permanent, it called for a permanent civil defense apparatus: `Like the Army, the Navy, and the Air Force, civil defense must function as long as a national security program is required.'

Id. at 49 (quoting Report of the East River Project: General Report, Part I I (1952).

The Cold War civil defense initiative was developed in response to a very different threat environment, and so cannot serve as a template for a cyber-threat control structure that integrates military personnel, law enforcement officers and civilians.[458] But, at the very least, it established a precedent for the type of civilian involvement in threat-control outlined above. My hope is that we can change the conversation in Washington to eliminate the recursive reliance on the fallacy of inevitability and move toward a more innovative, more effective approach to twenty-first century threats.

[458]Aside from anything else, civilians' role in the 1950s civil defense initiative was essentially limited to palliative efforts designed to minimize the harm inflicted by a nuclear attack. *See id.* at 33-77.