Cyber-threats and the Limits of Bureaucratic Control

Susan W. Brenner*

* Professor Brenner has spoken at numerous events, including Interpol Cybercrime Conferences, the Middle East IT Security Conference and the Yale Law School Conference on Cybercrime. She has also spoken on cyberthreats at the Department of Homeland Security's Global Cyber Security Conference, at a U.S. Department of State meeting on cybercrime and at a NATO Workshop on Cyberterrorism. In 2012, she chaired the Panel on Cyber-Security that was part of the American Society of International Law's Annual Meeting. She also presented a paper on state-sponsored economic espionage at the Harvard International Law Journal's 2012 symposium.

She has published a number of law review articles dealing with cybercrime, including *Fantasy Crime,* 11 Vanderbilt Journal of Technology and Entertainment Law 1 (2008). Oxford University Press has published two of her books: *Law in an Era of Smart Technology* (2007) and *Cyber Threats: Emerging Fault Lines of the Nation-State* (2009). And in 2010, Praeger published her most recent book: *Cybercrime: Criminal Threats from Cyberspace.* Her newest book—*Cybercrime and the Law: Challenges, Issues and Outcomes* was in the fall of 2012 by the University Press of New England.

Professor Brenner is also the author of the CYB3RCRIM3 blog, http://cyb3rcrim3.blogspot.com/.

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 modern nation-states rely on 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 Part 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

1. MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION 337 (Talcott Parsons ed., A. M. Henderson & Talcott Parsons trans., First Free Press Paperback Edition 1964) (1947).

2. I use the phrase "threat-control structures" to denote the institutional

course, not the first to make such an attempt. As I explain in Part 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.

Part 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 United States law and United States threat-control structures than I am with their correlates in other countries. 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, other countries,[3] which

---

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 Part II, they now also include cyber-variants of each threat, that is, cybercrime, cyberterrorism, and cyberwarfare. As Part 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. *See, e.g.*, *US Homeland Security & Defense Structure*, HOMELAND SECURITY RES. (Jan. 2010), http://www.homelandsecurityresearch.com/wp-content/uploads/2009/12/US-HLS-HLD-Structure-2010.pdf (diagramming the complex structure of the U.S.' threat-control initiatives). This chart only displays the federal agencies that are involved in the United States' threat-response and control effort. *See id.* As such, it encompasses law enforcement and military agencies, as well as agencies that engage in threat-control activities but do not fall neatly into either category, for example, the Central Intelligence Agency and National Security Agency. *See id.* Parts 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 United States 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* Henry Kenyon, *Army Cyber Unit Expands as Fast as It Can*, DEF. SYSTEMS (Feb. 25, 2011), http://defensesystems.com/articles/2011/02/28/cyber-defense-army-cyber-command.aspx (noting that headquarters of United States' new Cyber Command will "have a staff of more than 1,000 people when it is complete"), *with* Def. Manpower Data Ctr., *Active Duty Military Personnel Strengths by Regional Area and By Country*, U.S. DEP'T DEF. (Sept. 30, 2010), http://siadapp.dmdc.osd.mil/personnel/MILITARY/history/hst1009.pdf (showing the total U.S. active duty military personnel as of September 30, 2010 at 1,430,985 worldwide).

As to the size of U.S. law enforcement, 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. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ

suggests that the challenges it faces are likely to be more intractable than those that other countries confront.[4] In other

231174, LOCAL POLICE DEPARTMENTS, 2007 at 6 (2010); *see also Sheriffs' Offices*, BUREAU OF JUSTICE STAT., http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=72 (last visited Sept. 28, 2012) (noting that in 2008, 3,063 sheriffs' offices "had about 353,000 full-time employees, including 183,000 sworn officers"). A 2004 survey showed that the 49 "[p]rimary [s]tate" law enforcement agencies, for example, highway patrol and state troopers, had 89,265 full-time employees and 708 part-time employees. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 212749, CENSUS OF STATE AND LOCAL LAW ENFORCEMENT AGENCIES, at 2 (2007). And another roughly 60,000 officers were engaged in law enforcement at the federal level. *See* BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 212750, FEDERAL LAW ENFORCEMENT OFFICERS, at 2 (2006). From these somewhat dated reports it seems fair to estimate that state and local law enforcement agencies in the United States employ over 750,000 officers. Compare this number with the number of police in many countries. *See, e.g. Police Officers*, EUROSTAT, http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=crim_plce&lang=en# (last updated June 3, 2012) (noting number of police officers in European countries); *Sworn Police Officers in Australia*, AUSTRALIAN INST. CRIMINOLOGY, http://www.aic.gov.au/documents/9/C/B/%7B9CB4A373-91D5-4773-A57C-26F6E298F91F%7Dcfi116.pdf (last modified July 3, 2009) (noting 45,201 full-time police officers in Australia in 2004–2005). *But see China to Unify Police Identity Card from Jan. 1*, CHINA.ORG.CN, http://china.org.cn/english/news/194799.htm (last updated Jan. 1, 2007) (noting "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 several 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 nations usually have a single national police department that has authority over local units throughout the country."); *see also National Police Agency (NPA)*, FED'N AM. SCIENTISTS, http://www.fas.org/irp/world/japan/npa.htm (last updated Oct. 12, 2000, 9:50 AM) (indicating that The National Police Agency of Japan is the central coordinating body for the entire police system); *Responsibilities and Structure of Public Security Agencies in China*, MINISTRY PUB. SEC. CHINA, http://big5.mps.gov.cn/SuniT/www.mps.gov.cn/English/index.htm (last visited Oct. 8, 2012) (indicating that in China the Ministry of Public Security is in charge of security nationwide). And, as Part III notes, most countries do not have the rigid bifurcation between law enforcement and military initiatives that is found in the United States.

4. As James Q. Wilson notes 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 points 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, 18 FORDHAM INT'L L.J. 367, 374 (1994) (reviewing ETHAN A. NADELMANN, COPS ACROSS BORDERS: THE INTERNATIONALIZATION OF U.S. CRIMINAL LAW ENFORCEMENT (1993)).

> "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.

Id. (footnote 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, *Our Brave New Cyber World It's a Jungle Out There Let's Hope the President's New Cyber Czar Can Tame the Proliferating Threats to our Security*, PITTSBURGH POST-GAZETTE, June 7, 2009, at B1.

> [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.

Id.; *see also* Bruce Reed & Marc Dunkelman, Op-Ed., *Policing Our Cyberstreets*, BOS. GLOBE, Oct. 21, 2009, at A13 (noting that in dealing with "cybercrime and cyberterrorism, competition and turf wars between bureaucracies . . . frequently stymie the implementation of workable solutions"); Ryan J. Reilly, *Federal Agents Say Turf Wars Have Negatively Affected Investigations*, TPM MUCKRAKER (May 9, 2011, 3:56 PM), http://tpmmuckraker.talkingpointsmemo.com/2011/05/federal_agents_say_turf_wars_have_negatively_affec.php ("One-third of federal agents surveyed by a government oversight agency have gotten into turf wars with other federal law enforcement agencies during the course of an investigation. . . ."). *See, e.g.*, OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, AUDIT REPORT 11–22,

words, what is true for the United States is likely to be true for other countries as well.[5]

THE FEDERAL BUREAU OF INVESTIGATION'S ABILITY TO ADDRESS THE NATIONAL SECURITY CYBER INTRUSION THREAT at iv, 12–13 (2011), *available at* http://www.justice.gov/oig/reports/FBI/a1122r.pdf (illustrating a recent example of how inter-agency rivalries undermine the United States response to cyber-threats, noting the 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* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78–80, 91–92, 355–56 (2004) [hereinafter 9/11 COMMISSION REPORT]. See James B. Perrine et al., *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), for a summary of how and why information-sharing failed in the lead-up to the 9/11 attacks. See STEVEN K. O'HERN, THE INTELLIGENCE WARS: LESSONS FROM BAGHDAD 207–56 (2008), 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. 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." *Id.* at 211–12. 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. O'Hern explains that hubris arises because people believe their organization "can do more with the information" than if they share it with other organizations. *Id.* at 227.

Finally, as many have noted, bureaucracies are by nature risk-averse. *See, e.g.*, WILSON, *supra* note 4, at 69 ("[G]overnment 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, for example:

> Government agencies also 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.

9/11 COMMISSION REPORT, *supra* note 4, at 352; *see also* RALPH PETERS, BEYOND TERROR: STRATEGY IN A CHANGING WORLD 197 (2002) ("[B]ureaucracies discourage risk-taking or excellence that does not match the models of the past. The motto . . . is 'Play it safe.'").

5. For now and for the currently foreseeable future, this is most likely to be true for countries that (1) are frequent targets of cyber-attacks and (2) rely on the hierarchical response structures examined in Part II. As to the first factor, see, for example, TREND MICRO, THE BUSINESS OF CYBERCRIME: A COMPLEX BUSINESS MODEL 2 (2010), *available at* http://la.trendmicro.com/media/wp/cybercrime-business-whitepaper-en.pdf. *See*

As Part III explains, these proposals appropriately focus on remediating specific factors that contribute to the inefficacy with which current United States threat-control structures confront cyber-threats. As Part IV explains, 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 lateral, networked structures that prosper in cyberspace.[6] In Part V, I outline my thoughts as to how such a strategy could be structured and implemented.

II. THREATS

As Part III explains, cybercrime, cyberterrorism, and cyberwarfare differ from their real-world analogues in various ways, which means that strategies devised to deal with the latter may not be effectual in dealing with cyber-threats. To un-

---

also Matt Liebowitz, *'Oddjob' Trojan Sneaks into Your Bank Account*, NBCNEWS.COM (Mar. 14, 2011, 2:14 PM), http://www.msnbc.msn.com/id/41743730/ns/technology_and_science-security/t/oddjob-trojan-sneaks-your-bank-account (noting cybercriminals attacking targets "in the United States, Poland and Demark").

6. As to the non-hierarchical nature of cyber-threats, see, for example: "Few, if any, cyber-attacks occur in organizations with a formalized chain of command. Instead, multiple members of an organization . . . create a cyber-attack capability which is implemented on the decision of potentially different members. The system lacks a true hierarchy of decision making." Jonathan A. Ophardt, Note, *Cyber Warfare And The Crime Of Aggression: The Need For Individual Accountability On Tomorrow's Battlefield*, 2010 DUKE L. & TECH. REV. No. 3, ¶ 39. As to why hierarchical structures are not effective in dealing with cyber-threats, *see, e.g.*, CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 30 (2007) ("Cybercrime 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."); *see also* Reed Henry, *Enterprise Threat and Risk Monitoring Delivers the Rewards Without the Risk*, DATABASE AND NETWORK J., Apr. 2010, at 18, *available at* 2010 WLNR 11316176 ("[a] loosely-coupled and . . . well-organised group of players a cyber criminal can attack any size institution . . . .").

derstand 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.[7] This Part 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––city-states, empires, nation-states—must confront and overcome if they are to survive.[8] 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.[9]

Probably the greatest challenge societies confront is the need to maintain order, both internally and externally.[10] 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.[11] As failed states demonstrate, a society cannot survive if its members are free to prey on each other in ways that undermine the level of order needed to maintain a functioning society.[12] 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

---

7. See SUSAN W. BRENNER, CYBER-THREATS: THE EMERGING FAULT LINES OF THE NATION-STATE 13–23 (2009) [hereinafter CYBER-THREATS] for more on the traditional threat categories. *See also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Distributed Security*, 10 B.U. J. SCI. & TECH. L. 1, 5–64 (2004) [hereinafter *Criminal Law for Cyberspace*] (describing traditional threat categories).

8. *See Criminal Law for Cyberspace*, *supra* note 7, at 34–46. See also WEBER, *supra* note 1, at 156 for a summary of the characteristics of the modern nation-state.

9. *See Criminal Law for Cyberspace*, *supra* note 7, at 50–53.

10. *See id.* at 9–11, 34–46.

11. *See id.*

12. *See, e.g.*, Daniel Thürer, *The "Failed State" and International Law*, 836 INT'L REV. RED CROSS 731, 731–36, 740–42 (1999).

disruptive activity of some citizens.[13] To maintain order externally, a society must fend off encroachments and attacks by other societies.[14] To do this, a society must have trained personnel who are equipped with the weaponry they need to repel external attacks.[15]

1. Rules

Societies use two sets of rules to maintain internal order.[16] 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, divorce) and other equally critical matters.[17] Many civil rules are informal norms; most citizens internalize the norms and that keeps their behavior within socially acceptable bounds.[18] Other civil rules take the form of laws, the enforcement of which falls to civil courts and civil litigation (suits between individuals).[19]

Unlike other social species (e.g., ants, termites), humans are intelligent and can therefore deliberately decide not to follow a rule.[20] Most of the individuals in a society will not intentionally disobey the society's civil rules, but some will.[21] 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.[22] These rules are intended to discourage rule-violation by letting the state sanction those who commit "crimes."[23]

A crime consists of violating a rule—a law—that prohibits certain conduct or causing certain "harm."[24] Murder, for example, prohibits causing the death of another human being; theft

13. *See Criminal Law for Cyberspace*, *supra* note 7, at 9–11.

14. *See id.*

15. In other words, the state monopolizes the use of force in order to control threats that can disrupt order. *See* WEBER, *supra* note 1, at 156.

16. The discussion in this Part is adapted from *Criminal Law for Cyberspace*, *supra* note 7, at 9–60.

17. *Id.*

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.*

24. *Id.*

prohibits someone's taking another person's property without her permission and with the intention to deprive her of it.[25] 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.[26]

Criminal rules discourage rule violations by proscribing certain activity and by prescribing and inflicting sanctions on those who engage in it.[27] 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.[28] The sanction presumably deters enough would-be rule-violators to keep crime from undermining order in that society.[29]

This system assumes individuals commit crimes.[30] That assumption also applies to terrorism, which consists of committing what would otherwise be routine crime(s) for ideological reasons.[31] Criminals may commit crimes for financial reasons (e.g., fraud, theft) or passion (e.g., anger, sex).[32] The motive for committing crimes is personal: I steal to benefit myself; I murder out of revenge.[33] Terrorists commit crimes (e.g., killing peo-

---

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.*

29. *See* Susan W. Brenner & Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. MARSHALL J. COMPUTER & INFO. L. 659, 662 (2005) [hereinafter *Distributed Security*] ("[S]ocieties accept that they cannot eliminate it and so strive to control it.").

30. *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 No. 935, (1701) 88 Eng. Rep. 1518 (K.B.) ("A corporation is not indictable, but the particular members of it are."). And so far, humans seem to be the only "persons" who are committing cybercrimes and/or seem likely to commit cyberterrorism or engage in cyberwarfare. *See, e.g.*, Joshua Davis, *Web War One*, WIRED, Sept. 2007, at 162–69, 182–84.

31. *See, e.g.*, Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare,* 97 J. CRIM. L. & CRIMINOLOGY 379, 386–89 (2007) [hereinafter *At Light Speed*].

32. *See Criminal Law for Cyberspace*, *supra* note 7, at 57 n.331.

33. *See id.*

ple, damaging property) to promote an ideology.[34] Since terrorists commit crimes (albeit for distinct motives), societies have historically regarded terrorism as a type of crime.[35]

2. Territory

Historically, crime and terrorism were an internal phenomenon, i.e., both were committed within the territory of a sovereign entity,[36] such as a nation-state.[37] The internal character of crime/terrorism was a function of necessity: In the real-world, it is physically impossible for a person 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.[38]

War differs from crime and terrorism in two respects, one of which is that it is a struggle between sovereign entities.[39] While individuals wage war, warriors are merely implements; the players are the nation-states engaged in a political struggle.[40] War has been reserved for sovereign entities because only they could summon the resources (manpower, weapons) needed to wage war.[41] 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.[42] 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.[43] War has historically been an "outside" threat; crime and terrorism have been an "inside" threat.[44]

---

34. *See At Light Speed*, *supra* note 31, at 386–89.

35. *See id.* at 386 n.40.

36. See, e.g., CYBER-THREATS, *supra* note 7, at 13–18, for the link between territory and sovereignty. See WEBER, *supra* note 1, at 156, for a summary of the characteristics of the modern nation-state.

37. *See Criminal Law for Cyberspace*, *supra* note 7, at 105–06.

38. *See id.* at 39–56.

39. *See At Light Speed*, *supra* note 31, at 402–04.

40. *See* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1023 (2010).

41. *See* CYBER-THREATS, *supra* note 7, at 15–17.

42. *See id.* at 15–23.

43. *See id.*

44. *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.[45] These rules became the foundation of a strategy that has been effective in controlling real-space threats.[46] But as the Parts below explain, both the rules, and their enforcement 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.[47] While we may not have yet seen a verified incident of cyberterrorism, the same will be true of it as well.[48] 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 accurately categorize an attack as cybercrime, cyberterrorism, or cyberwarfare.[49]

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

---

45. *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, 1372–73 (2011).

46. Control is all societies strive for. *See Distributed Security*, *supra* note 29, at 662.

47. *See Criminal Law for Cyberspace*, *supra* note 7, at 69–70.

48. *See, e.g.*, CLAY WILSON, CONG. RESEARCH SERV., RL32114, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 7–9 (2008) (describing the 2007 Estonia cyber-attack).

49. *See, e.g.*, *id.*

one's physical characteristics limit the number and nature of identities he or she can assume.[50] 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.[51]

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.[52] 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.[53]

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.[54] 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).[55] 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.[56]

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.[57] 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.[58]

---

50. *See Criminal Law for Cyberspace*, *supra* note 7, at 65–66, 68–70.
51. *See id.* at 75.
52. *See id.* at 58–65.
53. *See id.* at 6.
54. *See id.* at 50–75.
55. *See id.*
56. *See id.*
57. *Id. at* 66–68; *see, e.g.*, Davis, *supra* note 30, at 162–69, 182–84.
58. *See Criminal Law for Cyberspace*, *supra* note 7, at 66–68.

2. External Threats

War is unambiguous in the physical world; when the Japanese attacked Pearl Harbor, there was no doubt this was war.[59] 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).[60] Another indicator was the weaponry itself, which was far beyond the capacity of individuals to acquire and utilize.[61]

We may or may not have seen instances of cyberwarfare.[62] We know, though, that it will not require the use of sophisticated, expensive weapons that can only be utilized by nation-states.[63] 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.[64]

All these factors erode the assumptions on which the three threat categories are based.[65] A cyber-attack that comes, or 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.[66] In cyberspace, states lose their monopoly on war and individuals lose their monopoly on crime and terrorism.[67]

This creates serious problems for countries like the United States, which rigidly bifurcate their threat response authority into (i) civilian (crime/terrorism) and (ii) military (war).[68] The bifurcation is predicated on the assumption that response personnel can easily distinguish crime/terrorism from war.[69] That

---

59. *At Light Speed, supra* note 31, at 406.

60. *Id.*

61. CYBER-THREATS, *supra* note 7, at 75.

62. *See* WILSON, *supra* note 48, at 7–9. *But see* CYBER-THREATS, *supra* note 7, at 85–90.

63. *See generally* CYBER-THREATS, *supra* note 7, at 75 (noting that weaponry used in traditional warfare is elaborate, and beyond the means of civilians to acquire).

64. *See, e.g.*, 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).

65. *See At Light Speed*, *supra* note 31, at 433–38.

66. *See id*.

67. *See id*.

68. *See id*. at 441–45.

69. *See id.* at 441.

premise is valid in the physical world, but, as explained below, is problematic for conduct vectored through cyberspace.

C. CYBERSPACE AND THREAT RESPONSE

This subpart 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 subpart 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,[70] and it is implicit in the laws governing crime and terrorism.[71] 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.[72] 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.[73] The clothing military attackers wear and the equipment they use display insignia indicating their national affiliation.[74] 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.[75]

Identifying those responsible for crime is usually much more difficult.[76] Criminals have a strong incentive to avoid identification because it is generally the first step toward being

---

70. *See, e.g.*, Matthew Hoisington, Note, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 451 (2009).

71. *See, e.g.*, *At Light Speed*, *supra* note 31, at 406–09.

72. CYBER-THREATS, *supra* note 7, at 127.

73. *Id.* at 128.

74. *Id.*

75. *Id.*

76. *Id.* at 128–29.

apprehended, convicted, and sanctioned for their misdeeds.[77] 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.[78]

This criminal investigation approach "assumes activity in the real world because, until recently, physical reality was the only arena of crime commission."[79] As noted above, this approach focuses on finding physical evidence at a crime scene and/or locating witnesses who saw the perpetrator.[80] It assumes the perpetrator was, and perhaps still is, in the local geographical area.[81] 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.[82]

Attacker-attribution for terrorism is more complicated than attack-attribution for war but less complicated than attack-attribution for crime.[83] 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.[84] However, "[i]f the sponsoring group does not claim credit for an attack, the structure and style of the attack may inferentially identify the organization responsible."[85] That may lead investigators to the individuals who carried out an attack.[86] 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.[87]

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 com-

77. *Id.*
78. *Id.* at 129.
79. *Id.*
80. *See id.*
81. *See id.*
82. *Id.*
83. *Id.* at 130.
84. *Id.*
85. *Id.*
86. *See id.*
87. *Id.*

puter systems.[88] BIS was forced to disconnect its computers from the Internet; it eventually discarded the infected computers and replaced them.[89] The attack was traced to sites hosted by Chinese Internet Service Providers (ISPs), but the attackers were never identified.[90]

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

The "place" of virtual attack 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 controlled by the attacker—in their assaults.[91] The "stepping stone" computers can be anywhere in the physical world because real-space is irrelevant to activity in cyberspace.[92] So while use of the Chinese servers might mean the attacks came from China, it might not mean that at all.[93] The attacker might be in Russia or Peoria.[94]

What if BIS-style attacks were repeated, with each coming from Chinese servers and targeting computers used by United States 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-

---

88. Alan Sipress, *Computer System Under Attack*, WASH. POST, Oct. 6, 2006, at A21.

89. *Id.*

90. *Id.*

91. *See* JEFFREY HUNKER ET AL., INST. FOR INFO. INFRASTRUCTURE PROT., ROLE AND CHALLENGES FOR SUFFICIENT CYBER-ATTACK ATTRIBUTION 6 (2008), *available at* http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

92. *See* CYBER-THREATS, *supra* note 7, at 131–40.

93. *See id.*

94. *See id.*

attribution. Assume that BIS-style attacks are launched against another United States agency's computers. Investigators trace these attacks to servers in Guangdong, China. For two years, sporadic attacks targeting United States civilian and government computers have been traced to Guangdong; some say Chinese military hackers conducted the attacks, others say Guangdong University students were responsible.[95] 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 that an attack originating in another nation-state was attributable to that nation-state.[96] If we apply this logic to the scenario above, the United States could rationally infer that the BIS-style attacks on United States 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.[97] The problem with this derivative inference of responsibility lies in equating an attack inferentially launched *from* Chinese territory with an attack launched *by* China.[98]

Historically, it was reasonable to equate transnational attacks with acts of war because only a nation-state could launch such an attack.[99] That is still true in the real-world, but cyberspace gives each nation-state an incremental, highly permeable

95. *At Light Speed*, *supra* note 31, at 410.
96. CYBER-THREATS, *supra* note 7, at 141–43.
97. *Id.*
98. *Id.*
99. *See id.* at 142.

set of "virtual" national borders.[100] Anyone with internet access and certain skills can launch a cross-border virtual attack on the cyberspace "presence" of an external nation-state.[101] A virtual attack is not territorially invasive, but it produces effects in the victim-state's territory that are damaging in various ways and in varying degrees.[102]

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.[103] 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.[104]

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.[105] 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.[106]

Point of attack origin therefore tends to be one, perhaps

---

100. *See id.*

101. *Id.* at 142–43.

102. *See, e.g.*, WILSON, *supra* note 48, at 7–9 (explaining large-scale sustained online attacks on Estonian infrastructure).

103. The discussion in this Part is adapted from CYBER-THREATS, *supra* note 7, at 143–61.

104. *Id.* at 143–44.

105. *Id.* at 144.

106. *Id.*

minor, factor in the processes law enforcement officers use to identify those responsible for crime and terrorism.[107] 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.[108] 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.[109]

As crime and terrorism migrate online, point of attack origin can assume more importance in attacker-attribution.[110] 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.[111] 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.[112]

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.[113] In these cases—for example, 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.[114]

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 oc-

---

107. *Id.* at 145.
108. *Id.*
109. *Id.*
110. *Id.*
111. *Id.* at 146.
112. *Id.*
113. *Id.* (citing Susan W. Brenner, *Should Criminal Liability Be Used to Control Online Speech?*, 76 MISS. L.J. 705 (2007)).
114. *Id.* (citing Paul Shukovsky, *Cyberstalker Just out of Reach of Law, But Finally, He Stops*, SEATTLE POST-INTELLIGENCER (Feb. 10, 2004, 10:00 PM), http://www.seattlepi.com/local/article/Cyberstalker-just-out-of-reach-of-law-but-1136722.php).

cupied by attacker and victim, in cyberspace, or in both?[115] For the purposes of attacker-attribution, the answer should be both.[116]

In "personal" attack cases, the connections between attacker and victim mean the parochial-attacker assumption is likely to be useful in identifying the attacker.[117] So far, cyber-vendettas seem primarily to originate in real-world contacts between attacker and victim.[118] 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.[119] The attack, then, should be construed as originating in the real-space occupied by attacker and victim.[120]

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.[121]

First, it serves an initial, essentially negative function in attacker-attribution.[122] 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.[123] 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.[124] Evidence, inferences, observations of witnesses and connections between victim and attacker all radiate from and revolve around this unitary crime scene.[125] It creates

---

115. *Id.* at 147.
116. *Id.*
117. *Id.*
118. *Id.* (citing Leroy McFarlane and Paul Bocij, *An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers*, FIRST MONDAY (Sept. 2003), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1076/996; *Online Harassment/Cyberstalking Statistics*, WORKING TO HALT ONLINE ABUSE, http://www.haltabuse.org/resources/stats/index.shtml (last visited Nov. 8, 2012)).
119. *Id.*
120. *Id.*
121. *Id.* at 148.
122. *Id.*
123. *Id.*
124. *Id.*
125. *Id.*

a comprehensible focus for the investigation and, in so doing, makes the investigation a manageable task.[126]

Second, cyberspace fractures the crime-scene into shards, the number of which depends on the particular circumstances of an attack.[127] 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.[128] 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.[129] The other constant shard, the omega shard, is the place of attack occurrence, which we examine below.[130]

Fracturing the crime scene into shards makes identifying the point of attack origin and linking it to the attacker much more difficult.[131] 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.[132]

Another issue that can complicate the process of backtracking through a series of incremental attack stages is the legal process involved.[133] Incremental attack stages will almost certainly involve the use of computers in different countries.[134] 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.[135] This process can be

---

126. *Id.*
127. *Id.* at 149.
128. *Id.*
129. *Id.*
130. *Id.*
131. *Id.*
132. *Id.*
133. *Id.* at 150–51 (citing Daniel A. Morris, *Tracking a Computer Hacker,* U.S. DEP'T OF JUSTICE, http://208.109.203.49/images/http_www.usdoj.gov_criminal_cybercrime_usamay2001_2.pdf (last updated May 3, 2005).
134. *Id.* at 151 (citing Tom Young, *IT Industry Core to Global E-Crime Battle*, COMPUTING (Nov. 9, 2006), http://www.computing.co.uk/ctg/analysis/1852053/it-industry-core-global-crime-battle).
135. *Id.* (citing Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence-Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 354–88 (2002)).

difficult, time-consuming, and even futile.[136] 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.[137]

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.[138] 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.[139]

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 cyber-attackers become more sophisticated about hiding their tracks.[140]

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."[141]

As with point of attack origin, the point of attack occurrence calculus becomes ambiguous when war migrates online.[142] Consider the BIS attacks: they occurred in the United States. What, if anything, does that tell us about who is responsible for them?[143]

We will assume the attacks originated in Guangdong, China.[144] Can we infer that cyber-attacks originating in China and occurring in the United States represent acts of war attributable to the Chinese government?[145] Unlike real-world acts of war, we do not have the presence of enemy personnel and ar-

---

136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.* at 152.
141. The discussion in this Part is taken from CYBER-THREATS, *supra* note 7, at 156–61.
142. *Id.* at 156.
143. *Id.*
144. *Id.*
145. *Id.*

mament on United States soil.[146] 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.[147] The signals bear neither state insignia nor other markers of nation-state allegiance.[148] 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 United States government computers).[149]

We have already analyzed the ambiguity involved in determining point of attack origin.[150] Here, the point of attack occurrence is not ambiguous; we know it occurred in the United States.[151] The ambiguity lies in the implications of this point of occurrence.[152] 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.[153] 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.[154]

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.[155] Real-world trans-border attacks have been equated with war because only nation-states could launch such attacks.[156]

Cyberspace changes that: we cannot infer from the mere fact that the attacks targeted computers on United States soil that they are the equivalent of Hitler invading Poland.[157] In utilizing point of attack occurrence in attacker-attribution, we must modify the assumption that equates trans-border attacks with war so it incorporates a basic reality of the online envi-

---

146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.* at 157.
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*
156. *Id.*
157. *Id.*

ronment: United States government and civilian computers are attacked because they are attractive targets for criminals, terrorists, and, ultimately, perhaps, nation-states bent on war.[158] Since United States computers are attractive targets for all three categories of attackers, any of whom can launch trans-border 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.[159]

That brings us to crime/terrorism: point of attack occurrence is an integral component of attacker-attribution for both.[160] Investigations concentrate on the place where the attack occurred.[161] 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.[162]

Thus, point of attack occurrence plays a central role in investigating these real-world events.[163] 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.[164] 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.[165] The place where the attack occurs is sometimes itself a source of inference as to the identity of an attacker.[166] If someone is murdered in a home with an armed alarm system, this suggests the attacker knew the victim.[167]

Here, again, the importance of point of attack occurrence diminishes as attacks move online.[168] 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 en-

158. *Id.*
159. *Id.* at 157–58.
160. *Id.* at 159.
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.*
167. *Id.*
168. *Id.*

try to a computer hooked to a cable modem does not.[169] 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.[170] 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.[171]

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).[172] 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.[173] 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.[174]

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.[175] 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.[176] External order was a purely sovereign concern; nation-states challenged each other in the international arena and resolved matters with military combat.[177] Non-state actors were limited to challenging a state's ability to maintain internal order, i.e., by committing crimes or acts of terrorism. This changes as activities move

169. *Id.*
170. *Id.* at 160.
171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.*
175. *See supra* Part II.C.1.
176. *See supra* Part II.C.1.
177. *See supra* Part II.C.1.

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.[178] 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).[179]

Real-world terrorism is usually easy to identify though it often involves activity that would otherwise constitute crime.[180] 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.[181]

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.[182] 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.[183]

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 United States government computers and originated in China, perhaps in Guangdong, which may be associated with China's cyberwar effort.[184]

The circumstances of the attacks suggest they were a sortie

---

178. CYBER-THREATS, *supra* note 7, at 76.

179. *Id*. at 21.

180. *Id*. at 76.

181. *See id.* at 40–41 (noting that terrorism is meant to serve ideological purposes and make civilians feel vulnerable).

182. *Id*. at 75.

183. *Id*.

184. The discussion in this Part is adapted from *At Light Speed*, *supra* note 31, at 434–38.

into cyberwar.[185] 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;[186] this presumption suggests the BIS attacks were war.[187] 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.[188]

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 United States government computer systems.[189] 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.[190] 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.[191] 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 United States government.[192] For years Guangdong has been producing hackers, and for years civilian hackers of various nationalities have been exploring United States government computers.[193] It is as possible that the attacks came from student hackers in Guangdong as it is that they came from the Chinese government.[194]

What if a BIS-style attack targeted a corporate computer

---

185. *Id.* at 434.

186. *See supra* Part II.C.1.b.

187. *At Light Speed*, *supra* note 31, at 435.

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. *Id.* (citing *Is China Ground Zero for Hackers?*, ZDNET (Aug. 29, 2001, 12:00 AM), http://www.zdnet.com/news/is-china-ground-zero-for-hackers/96486).

193. *Id.* (citing Colin Barker, *The NASA Hacker: Scapegoat or Public Enemy?*, ZDNET (July 13, 2005, 12:35 PM GMT), http://www.zdnet.com/the-nasa-hacker-scapegoat-or-public-enemy-3039208862/).

194. *Id.* (citing *Is China Ground Zero for Hackers?*, ZDNET (Aug. 29, 2001, 12:00 AM), http://www.zdnet.com/news/is-china-ground-zero-for-hackers/96486).

system?[195] The nature of the target inferentially suggests it was cybercrime, as we assume criminals attack other civilians.[196] That conclusion would be reinforced if the attackers' actions conformed to what we expect of cybercriminals, for example, if they extracted funds from corporate accounts or personal information from databases.[197] Since we assume civilians are the targets of crime, not war, an attack such as this would almost certainly be construed as cybercrime.[198]

Relying too heavily on this assumption could be a mistake.[199] The attack on a corporate entity could be cyberwar, not cybercrime.[200] China's focus on cyberwar includes attacks on civilian entities.[201] 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.[202]

An analogous, but perhaps less serious, problem arises if the attack on our corporate entity is cyberterrorism.[203] 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 or temporally, or both, and that have different points of origin.[204] 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.[205] 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.[206]

This problem arises because of our partitioned responsibility for responding to crime/terrorism versus warfare and be-

195. *Id.* at 436.
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.* at 437.
200. *Id.*
201. *Id.*
202. *Id.*
203. *Id.*
204. *Id.*
205. *Id.*
206. *Id.*

cause we tend to assume crime is a localized phenomenon.[207] 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.[208] 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 (iii) motive for an attack.[209]

As we have seen, the utility of the first two markers erodes as attacks migrate online.[210] The same is also true, but in a different way and for different reasons, for the third factor.[211] 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.[212] Motive is and will continue to be a valid differentiating factor for cyber-attacks: profit drives most crime, ideology drives terrorism, and nation-state rivalries have historically driven warfare.[213] 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.[214]

We know what the BIS attackers did, but we cannot ascertain why they did it.[215] 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 or revenge), that may not always be true.[216] Terrorists, for example, are increasingly using cybercrime to finance their real-world efforts, which give us a mixed-motive scenario: the

---

207. *Id.*
208. *Id.* at 438.
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.* (citing Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME, Sept. 5, 2005, at 34).

motive for committing cybercrimes is profit, a criminal motive, but the motive for obtaining the profit is to engage in acts of terrorism, a noncriminal motive.[217] It is also increasingly possible that nonstate actors could commit cybercrimes to obtain the money needed to launch cyber-attacks 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.[218] 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.[219]

The efficacy of both strategies depends on a state's ability to respond effectively to a threat.[220] 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.[221] As noted above, many countries—particularly the United States—use a bifurcated response system: Law enforcement responds (only) to internal threats (crime or terrorism), and the military responds (only) to external threats (war).[222] The bifurcation is a function of both 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).[223]

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

---

217. *Id.*

218. *Id.* at 430.

219. *See* CYBER-THREATS, *supra* note 7, at 165–74.

220. The discussion of threat response tactics is adapted from CYBER-THREATS, *supra* note 7, at 163–99.

221. *Id.* at 184.

222. *See id.* at 164–76.

223. *See* THE MILITARY IN THE SERVICE OF SOCIETY AND DEMOCRACY: THE CHALLENGE OF THE DUAL-ROLE MILITARY 4–5 (Daniella Ashkenazy ed., 1994). *But see* DIANA CECELIA WEBER, CATO INST, BRIEFING PAPER NO. 50, WARRIOR COPS: THE OMINOUS GROWTH OF PARAMILITARISM IN AMERICAN POLICE DEPARTMENTS 2 (1999) (the war on drugs encouraged the "militarization of law enforcement in America").

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, such as the air traffic control system. The agents conclude the attacks are coming from a location in China that is associated with both China's military preparation for cyberwar and university student hackers. If the attacks are cybercrime or cyberterrorism, the FBI can and must respond to them.[224] If they constitute war, the United States military must

---

224. 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. *See At Light Speed*, *supra* note 31, at 430. 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 United States targets. It might want to intervene, just as FBI agents intervene when they encounter a real world crime in progress.

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 United States 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 sig-

respond.

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 or 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.[225] The FBI is certain that the attacks target a United States government agency and, consequently, threaten serious harm to United States 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 United States military personnel, because of the bifurcation noted earlier, i.e., under United States law, military personnel cannot participate in law enforcement.[226]

The FBI could presumably alert the military to the occurrence of the attacks and let the military conduct its own as-

---

nals 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 or attack the computers from which they originate, or both, this would constitute a crime under Chinese law, which means China could legitimately demand that the United States turn the agents over to be prosecuted in China. *See* PROJECT ON CYBERCRIME, COUNCIL OF EUROPE, CYBERCRIME LEGISLATION—PEOPLE'S REPUBLIC OF CHINA 10 (2008) [hereinafter PROJECT ON CYBERCRIME], *available at* http://www.coe.int/t/dg1/legalcooperation /economiccrime/cybercrime/Documents/CountryProfiles/567-LEGcountry%20profile%20China%20PR%20_28%20Mar%2008_.pdf. An FBI investigation conducted some years ago prompted such a response. *See, e.g.*, *FSB Hopes to Bring to Court Case against FBI Agents*, INTERFAX, Oct. 10, 2002, *available at* 2002 WLNR 14527663; *Russia: FSB Charges FBI with Hacking*, INFOPROD, Aug. 25, 2002, *available at* 2002 WLNR 3203882.

225. *See supra* Part II.C.2.b.

226. *See* CYBER-THREATS, *supra* note 7, at 17–18, 177–78.

sessment of the nature of the attacks and need for and propriety of the military responding to them. To avoid the need to consider whether such action would violate any aspect of United States 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.[227] Since 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.[228]

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

---

227. 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 224. 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 supra* note 224. The fact that agents of the United States 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 United States 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. *See supra* Part II.A.2; *At Light Speed*, *supra* note 31, at 402, 433.

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.*, Brenner & Clarke, *supra* note 40, at 1022–23.

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. If Chinese officials did not, the FBI could 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 224.

228. *See* Brenner & Clarke, *supra* note 40, at 1030–31 (explaining that Article 2(4) of the United Nations Charter "outlaws aggressive war").

the circumstances, the Chinese government may argue (perhaps quite accurately) that it was not responsible for the attacks that resulted in the United States military's attacking computer systems in China. If China truly was not responsible for the attacks, the United States military's response will constitute offensive cyberwarfare; and since offensive warfare is unlawful under the laws of warfare, it has committed an illegal act.[229]

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 respond effectively to a threat ultimately depends on its ability to reliably and expeditiously ascertain what type of threat is at issue. As the Parts 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.[230] That, in turn, erodes a nation-state's ability to deter and thereby control cyber-threats.

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 seg-

---

229. *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* PROJECT ON CYBERCRIME, *supra* note 224, at 10.

230. It can also reduce the effectiveness of responses by delaying them until some or all of the intended harm has been inflicted. *See* CYBER-THREATS, *supra* note 7, at 94–98.

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

regate 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 respond effectively to cyberthreats. Part III examines some efforts that seek to do precisely this.

III. IMPROVED THREAT CONTROL: CURRENT EFFORTS

[O]ur cyber-defenses are woefully lacking.[231]

The discussion in Part 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 those of other countries.[232] 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.[233]

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, often overlapping, agendas.[234] 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."[235] 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

---

231. Mike McConnell, *To Win the Cyber-war, Look to the Cold War*, WASH. POST, Feb. 28, 2010, at B1.

232. *See supra* note 3 and accompanying text.

233. *See supra* notes 3–4 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).

234. 9/11 COMMISSION REPORT, *supra* note 4, at 399–403; *see also id. at* 73–102 (describing the roles of each agency).

235. *Id.* at xvi.

nation-states and call for quick, imaginative, and agile responses."[236] 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 such "quick, imaginative, and agile responses" is not limited to the real-space terrorism context. The parts below therefore examine three efforts to meet this need in the context of cyberthreats.

A. CYBER COMMANDS

This subpart examines how the U.S. military is attempting to improve its efficacy in dealing with the cyberthreats that currently fall within its area of responsibility.[237] As I explain 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 to establish U.S. Cyber Command,"[238] which achieved "Initial Operational Capability" on May 21, 2010.[239] This particular Cyber Command is "a sub-unified command" that is "subordinate to U.S. Strategic Command" and 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.[240]

To appreciate why Cyber Command was (apparently) established, it is necessary to understand how its subsidiary

---

236. *Id.* at 399.

237. As Part II explained, the military is responsible for protecting the nation from external attacks launched by hostile nation-states.

238. *U.S. Cyber Command*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/cyber_command (last updated Dec. 2011). The U.S. Strategic Command is "a unified command" that is designed "to adapt to the changing international political and military landscape . . . ." *Frequently Asked Questions*, U. S. STRATEGIC COMMAND, http://www.stratcom.mil/faq (last visited Nov. 5, 2012).

239. *U.S. Cyber Command*, *supra* note 238.

240. *Id.* Interestingly, the Cyber Command "fact sheet" only lists the first four entities (Air Force, Army, Navy, and Marines) as Cyber Command subunits. *Id. But see* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 5 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf (indicating that Coast Guard Cyber Command is part of U.S. Cyber Command). I will assume the Coast Guard Cyber Command is, indeed, a Cyber Command component.

commands came into existence. The process began in 2005 when the Air Force amended its Mission Statement to state that it will "fly and fight" in cyberspace, as well as in air and space.[241] 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.[242] At the time, it seemed the Air Force was staking out responsibility for cyberspace, just as it had earlier done for "air" and "space."[243] Then the Air Force put the project on hold to "make a fresh assessment" of the proper approach to establishing a cyber command.[244] On August 19, 2009, Air Force Cyber Command became part of the Air Force Space Command.[245]

The Marine Corps' Cyberspace Command was established on January 21, 2010 to protect and defend "the nation's cyber-infrastructure."[246] It "join[ed] a growing list of [Department of Defense] agencies now tasked to support the government's Cyber Command effort."[247] 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.[248] It "provid[es] operational support to

---

241. *See* Mitch Gettle, *Air Force Releases New Mission Statement*, AF.MIL (Dec. 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.*

242. *See* RICHARD MESIC ET AL., RAND CORP., AIR FORCE CYBER COMMAND (PROVISIONAL) DECISION SUPPORT at iii (2010), *available at* http://www.rand.org/pubs/monographs/2010/RAND_MG935.1.pdf; Todd Lopez, *Air Force Leaders to Discuss New 'Cyber Command,'* AF.MIL (Oct. 5, 2006), http://www.af.mil/news/story.asp?id=123028524.

243. *See* C. Todd Lopez, *Cyber Summit Begins at Pentagon Nov. 16*, AF.MIL (Nov. 15, 2006), http://www.af.mil/news/story.asp?id=123032005 (noting "[c]yberspace became an official Air Force domain, like air and space, on Dec. 7, 2005" when the new Mission Statement was introduced).

244. *On Pause, But Not Abandoning,* AIRFORCE-MAGAZINE.COM (Aug. 14, 2008), http://www.airforce-magazine.com/DRArchive/Pages/default.aspx (follow "2008" hyperlink; then follow "Thursday, August, 14, 2008" hyperlink).

245. Carla Pampe, *Air Force Activates Cyber Numbered Air Force*, 24TH AIR FORCE (Aug. 19, 2009), http://www.24af.af.mil/news/story.asp?id=123163975.

246. Alan J. McCombs, *Marines Launch into Cyberspace Mission with New Command*, ARMY.MIL (Jan. 28, 2010), http://www.army.mil/article/33744/Marines_launch_into_cyberspace_mission_with_new_command.

247. *Id.*

248. *Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet*, NAVY.MIL (Jan. 29, 2010, 6:48 PM), http://www.navy.mil/search/display.asp?story_id=50954.

Navy commanders worldwide" for "information and computer network operations, electronic warfare and space."[249] The Coast Guard's Cyber Command was created in June or July 2010.[250] Its mission is to protect Coast Guard computer systems and data, to aid in Coast Guard missions, and to protect the marine transportation system and critical infrastructure from cyber-attacks.[251] Finally, on October 1, 2010 the Army established its Cyber Command that "plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks."[252]

To an observer, it might seem peculiar that all five branches of the United States 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

---

249. Joseph E. Sisson, Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort 14 (May 3, 2010) (unpublished student work, Naval War College), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA525307.

250. *See* Amber Corrin, *Cyber Command Lays Groundwork for Rapid Deployment of Resources*, GOV'T COMPUTER NEWS (July 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*, DEF. DAILY, May 6, 2010, *available at* 2010 WLNR 10703214. *See generally* U.S. DEP'T OF DEF., *supra* note 240, at 5 (noting the existence of the Coast Guard Cyber Command and its inclusion in Cyber Command).

251. A 2011 article noted that the Coast Guard Cyber Command was then "still in its infancy and awaiting a final stamp of approval." Eric Beidel, *Coast Guard Cyberdefense Office: Small But Mighty*, NAT'L DEF. (Nov. 2011), http://www.nationaldefensemagazine.org/archive/2011/November/Pages/CoastGuardCyberdefenseOfficeSmallbutMighty.aspx. More interestingly, the article notes:

> Navy ships often carry Coast Guard detachments because the larger service can't board vessels for law enforcement purposes. Officials are pondering what the equivalent of such actions would be in cyberspace. The smallest service's title authorities place it at the crossroads of defense, homeland security and law enforcement missions. That versatility could prove crucial to a government that is still trying to figure out exactly how it should handle the spectrum of operations in cyberspace, officials say. After all, there may be situations when U.S. Cyber Command just can't pull the trigger on a law enforcement measure, but the Coast Guard can.

Id. This aspect of the Coast Guard Cyber Command's mission may explain why its role in the nation's cybersecurity efforts has received little, if any, publicity since it was created.

252. *Army Cyber*, U.S. ARMY CYBER COMMAND, http://www.arcyber.army.mil/org-arcyber.html (last visited Sept. 28, 2012).

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.[253] 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).[254] 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.[255]

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 United States Army, evolved to fight land battles; navies, like the United States Navy, evolved to fight sea battles;[256] the United States Marines evolved as an amphibious fighting force;[257] the United States Coast Guard was created to control smuggling and has evolved into a maritime law enforcement agency that can also perform military functions;[258] and the U.S. Air Force evolved to conduct military operations in the air.[259]

---

253. *See, e.g.*, *CIA Official Says Cybersecurity Threats Evolving Faster than Defense*, INSIDE PENTAGON, (July 29, 2004), *available at* 2004 WLNR 82077; *U.S. Government Well Defended against Cyber-Attacks, State Says*, U.S. DEP'T OF ST. (Aug. 26, 2005), http://iipdigital.usembassy.gov/st/english/texttrans/2005/08/20050826145518tjkcollub0.7742426.html#axzz28CEVskw7; Gerald Sonnenberg, *Communicators Train to Face Enemies on Digital Battlefield*, AF.MIL (Dec. 13, 2004), http://www.af.mil/news/story.asp?id=123009398.

254. *See* Robert F. Dorr, *New Mission Statement Isn't Really for Airmen*, AIR FORCE TIMES, Dec. 26, 2005, at 38.

255. *See id.* (stating that the 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*, NAT'L J., Nov. 14, 2009, at 18, 22 (explaining that the four branches "competed with one another to control the military's overall strategy"); Kevin Coleman, *Inside the Cyber Command Turf Battle*, DEF. TECH (Aug.15, 2008), http://defensetech.org/2008/08/15/inside-the-cyber-command-turf-battle.

256. *See* Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 314 (2008).

257. *See Mission*, THEUSMARINES.COM, http://www.theusmarines.com/mission (last visited Nov. 5, 2012).

258. *See Missions*, USCG.MIL, http://www.uscg.mil/top/missions (last visited Nov. 5, 2012).

259. *See History*, AIRFORCE.COM, http://www.airforce.com/learn-about/history (last visited Nov. 5, 2012).

This segmentation of responsibility for responding to external threats is a logical strategy in a world in which threats are territorially based.[260] In that world, the response to an external threat, e.g., the Japanese attack on Pearl Harbor, focuses on a 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 nonmilitary activities, but it is officially a branch of the United States armed services and operates under the authority of the Navy when the country is at war.[261]

As we saw in Part 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[262] threat response approach is still viable in the twenty-first century. If it is still viable, the second issue is how the bifurcated approach can be reconfigured to improve the United States' approach to defending against cyber-threats.

We will not address the first 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 satisfactory way to control these threats, which will persist.[263] It would

260. *See supra* Part II.

261. *See* 14 U.S.C. § 1 (2006); *see also Missions*, *supra* note 258.

262. 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* Part II.

263. As to why they will persist, see, e.g., *Criminal Law for Cyberspace*, *supra* note 7, at 45–46. 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 intrasovereign conflicts will continue to emphasize kinetic force, as well as

therefore be imprudent to decide that 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.[264] 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, 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 Part 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.[265] I think the preferable course is to concede that the bifurcated approach, as it is currently configured, is not effective against cyber-threats and then analyze how it can be reconfigured to improve its efficacy in this regard.

---

cyberforce, at least to the extent that one sovereign seeks to expand its control over physical territory and assets.

264. As to why the approach is not effective in controlling cyber-threats, see *supra* Part II.

265. Relying on a unitary entity to conduct both law enforcement and military functions would violate federal law and, perhaps, the Constitution. *See* CYBER-THREATS, *supra* note 7, at 164–76.

I see this as the most pressing, and more manageable, of the two issues. The remainder of this Part undertakes the first task noted above: it reviews how the U.S. structures the bifurcated approach and analyzes the extent to which this impedes the country's response to cyber-threats. Part III.A.2 examines the military, Part III.B examines law enforcement, and Part III.C reviews proposed legislation that is designed to incorporate civilian participation into the efforts of either or both. Part IV 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.[266] 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 flies in cyberspace.[267]
- The Marine Corp's cyber command defends the nation's cyberinfrastructure.[268]
- The Navy's cyber command provides operational support to Navy commanders engaged in cyberwarfare.[269]
- The Coast Guard's cyber command protects the marine transportation system and critical infrastructure from cyberwarfare.[270]
- The Army's cyber command plans, coordinates, and conducts cyberwarfare.[271]

As noted in Part 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 con-

266. *See supra* Part III.A.1. From this point forward, I will use "cyber command" to denote one of the branch cyberunits and "Cyber Command" to denote the overarching entity.

267. *See* Dorr, *supra* note 254.

268. *See* McCombs, *supra* note 246.

269. *See* Sisson, *supra* note 249, at 14.

270. *See* Beidel, *supra* note 251.

271. *See Army Cyber*, *supra* note 252.

tributions are not, of course indistinguishable. In wartime four of the branches (Air Force, Army, Marine Corps, and Navy) have a specific, complementary role to play, and the Coast Guard becomes part of the Navy.[272]

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 contributions each will make to that effort.[273] The Marine Corps' and Coast Guard's mission statements can be interpreted the same way.[274]

This inferentially suggests that there is no doctrinal or operational differentiation among the roles the respective commands would play in cyberspace.[275] The validity of that inference is further supported by the fact that "cyberspace" denotes an experiential, rather than spatial, phenomenon.[276] There is,

---

272. *See supra* notes 256–261 and accompanying text.

273. *Cf. supra* notes 267, 269, 271 and accompanying text.

274. *Cf. supra* notes 268, 270 and accompanying text. One *could* argue that by pledging to defend or protect the country's critical infrastructure the Marine Corps and the Coast Guard might be pledging to utilize kinetic force, as well as cyberforce, in this regard. The other mission statements seem to contemplate only nonkinetic activity. For the present, there is, at least, a tacit assumption that cyberforce will be met only with cyberforce, to avoid the risks of escalating a digital conflict into something more devastating. *See Cyber Warfare: Rising Risks and Implications*, EMERGING MARKETS ONLINE, Sept. 13, 2010, *available at* 2010 WLNR 18254196; Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C. J.L. & TECH. ONLINE 1, 18–24 (2010) (discussing responding to and retaliation against cyber-attacks).

275. *See* Eric Beidel, *Disjointed, Redundant Cybersecurity Programs Undermine Efforts to Protect Networks*, NAT'L DEF. (July 18, 2011, 10:54 AM), http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=470; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-421, DEFENSE DEPARTMENT CYBER EFFORTS: MORE DETAILED GUIDANCE NEEDED TO ENSURE MILITARY SERVICES DEVELOP APPROPRIATE CYBERSPACE CAPABILITIES 17 (2011) ("The military services 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.").

276. *See* Joseph Schmitt & Peter Nikolai, *Application of Personal Jurisdiction Principles of Electronic Commerce: A User's Guide*, 27 WM. MITCHELL L. REV. 1571, 1577–78 (2001) (referring to William Gibson's use of "cyberspace" to refer to "the non-existent space where computer communication takes

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 problem.[277] 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."[278]

Cyber Command has so far made little progress toward achieving this goal.[279] In 2011 the Government Accountability Office issued a report in that was strongly critical of 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."[280] A spokesman for Cyber Com-

---

place"); WILLIAM GIBSON, NEUROMANCER 51 (Ace Books 2000) (describing cyberspace as a "consensual hallucination experienced daily by billions of legitimate operators . . . . A graphic representation of data abstracted from the banks of every computer in the human system").

277. *See U.S. Cyber Command*, *supra* note 238 ("The Command centralizes direction of cyberspace operations . . . .").

278. Seymour M. Hersh, *The Online Threat*, NEW YORKER, Nov. 1, 2010, at 44, 46. Cyber Command's designated tasks are to lead "day-to-day defense and protection of [Department of Defense] information networks; coordinate DoD operations providing support to military missions; direct the operations and defense of specified DoD information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations." *U.S. Cyber Command Fact Sheet*, U.S. DEP'T DEF. (May 25, 2010), http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

279. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 275, at 17 (May 2011) (commands "are pursuing diverse service-specific approaches to establishing cyberspace capabilities because . . . Cyber Command has . . . not fully defined long-term mission requirements and capabilities."); *see also Army Cyber Command*, 2011 ARMY POSTURE STATEMENT (last updated Mar. 21, 2011, 3:44 PM), https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/information_papers/PostedDocument.asp?id=256 (describing how the army cyber command has incorporated "existing cyberspace 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).

280. Lolita C. Baldor, *Report Says Pentagon Should Boost Cyber Staff*, AIRFORCETIMES (June 20, 2011, 5:26 PM), 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 Fogarty, *Is It Time for the Pentagon to Turn Cyberwar Over to Someone Else?*, ITWORLD (July 29, 2011, 12:00 AM), http://www.itworld.com/node/187699?source=cotd. "The overall picture the

mand said it was addressing these issues, but "there is currently no 'timeline for completion.'"[281]

Before Cyber Command was created, some members of the military argued that branch-specific commands could not provide an effective cyberwar response system.[282] They claimed the "cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare."[283] And they contended that the "core skills" needed to wage cyberwar differ radically from those needed for conventional war.[284] 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.[285]

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 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.[286] 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.[287]

Cyberspace operations do not take place in a physical

GAO paints is of fragmented military organization with no clear direction or goal to pursue in cybersecurity." *Id.*

281. Tiffany Kaiser, *GAO Report: Pentagon Must Provide Better Training for New Cyber Command Security System*, DAILY TECH (June 21, 2011, 12:13 PM), http://www.dailytech.com/GAO+Report+Pentagon+Must+Provide+Better+Training+for+New+Cyber+Command+Security+System/article21963.htm.

282. *See, e.g.*, Gregory Conti & John "Buck" Surdu, *Army, Navy, Air Force, and Cyber—Is It Time for a Cyberwarfare Branch of Military?*, 12 IANEWSLETTER 14, 16 (2009), *available at* http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf.

283. *Id.*

284. *See id.*

285. *See id.* at 17.

286. *See supra* Part III.A.1.

287. *See supra* Part III.A.1.

place; instead, they involve activity that occurs in and through computer technology, which is pervasive in today's world.[288] 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 cyberbranch 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 cyberbranch 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 cyberbranch would essentially subsume the other branches as to its distinct area of responsibility. That could be problematic. It might, for example, create clashes of authority that could have negative consequences for the United States' ability to respond to cyberattacks.[289]

This might be one of the reasons the Department of Defense 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 activi-

---

288. *See, e.g.*, *At Light Speed*, *supra* note 31, at 401 ("Cyberwarefare is the conduct of military operations by virtual means.").

289. Assume, say, that a hostile state's own cyberwarriors use "cyberattacks to alter data, such as logistics plans" stored in United States military computers. Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 389 (2011). Assume the plans at issue were created by and are to be used by the United States Army; also assume that the hypothesized United States 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.

ties 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 United States military's conventional Unified Combatant Commands.[290] These Commands incorporate personnel from the five military branches into a unified command with responsibility for a specific geographical area.[291] 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.[292]

As we saw above, cyberspace, unlike real space, cannot be parsed into spatial domains.[293] Unless 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.[294] 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.[295]

There is yet another issue Cyber Command must resolve. Since the task list cited earlier 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

---

290. *See, e.g.*, *Unified Command Plan*, DEFENSE.GOV, http://www.defense.gov/home/features/2009/0109_unifiedcommand (last updated Apr. 27, 2011).

291. *See, e.g.*, U.S. AFRICOM Pub. Affairs Office, *Fact Sheet: United States Africa Command*, U.S. AFR. COMMAND (May 24, 2012), http://www.africom.mil/getArticle.asp?art=1644.

292. *See, e.g.*, *id.*

293. *See supra* Part II.

294. *See supra* Part III.A.2; *see also* Kaiser, *supra* note 281. 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* U.S. DEP'T OF DEF., *supra* note 240.

295. *See supra* notes 279–281 and accompanying text; *see also* Kathleen Hickey, *DOD's Cyber Strategy Lacks Organization, Manpower and Funds, GAO Says*, GOV'T COMPUTER NEWS (July 26, 2011), http://gcn.com/articles/2011/07/26/dod-cyber-strategy-weaknesses-gao.aspx.

protecting military assets and networks. In other words, would Cyber Command also be responsible for protecting civilians and civilian-owned assets?[296]

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.[297] This caused controversy because, as Part 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 was 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.

In testifying before the House Armed Services Committee, General Alexander prosposed that Cyber Command "could also have a broader role in the civilian sector through protecting US critical infrastructure networks and systems."[298] 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."[299] A few days later, the Department of Defense and the Department of Homeland Security[300] perhaps sought to address this issue, at least in

---

296. Hersh, *supra* note 278, at 49.

297. Noah Shachtman, *Military's Cyber Commander Swears: "No Role" in Civilian Networks*, WIRED.COM (Sept. 23, 2010, 10:00 AM), http://www.wired.com/dangerroom/2010/09/militarys-cyber-commander-swears-no-role-on-civilian-networks.

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

299. *Id.* However, Alexander later backed away from his request for additional legal authority. Ellen Nakashima, *Cyberattacks Should Require Presidential Authorization, Official Says*, WASH. POST, Mar. 27, 2012, http://www.washingtonpost.com/world/national-security/cyberattacks-should-require-presidential-authorization-official-says/2012/03/27/gIQA0312eS_story.html. As noted earlier, under U.S. law the military is barred from participating in law enforcement efforts. CYBER-THREATS, *supra* note 7, at 164–76.

300. The Department of Homeland Security is charged with protecting citizens of the United States from internal threats, especially terrorism. *See, e.g.*, DEP'T OF HOMELAND SEC., ONE TEAM, ONE MISSION, SECURING OUR HOMELAND: U.S. DEPARTMENT OF HOMELAND SECURITY STRATEGIC PLAN

part, by signing a memorandum of understanding that (i) gives Homeland Security "lead responsibility for protecting the United States 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 non-state actors."[301]

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 U.S.'s ability to mount a unified response to cyber-threats. The primary constraint is the bifurcation described in Part II: the military (Defense) deals with war, while law enforcement (Homeland Security)[302] deals with crime and terrorism. Due to historical circumstance, the bifurcation

---

FISCAL YEARS 2008–2013 at 2–3 (2008), *available at* http://www.hsdl.org/?view&did=235371.

301. Donna Miles, *DOD, Homeland Security Collaborate in Cyber Realm*, INFOWARS.COM (June 3, 2011), http://www.infowars.com/dod-homeland-security-collaborate-in-cyber-realm; *accord* Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity (Sept. 27, 2010), *available at* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf; *see also* Press Release: U.S. Dep't of Homeland Sec., Joint Statement by Secretary of Defense Robert Gates and Secretary of Homeland Security Janet Napolitano on Enhancing Coordination to Secure America's Cyber Networks (Oct. 13, 2010), *available at* http://www.dhs.gov/ynews/releases/pr_1286984200944.shtm; *Cybersecurity: Assessing the Immediate Threat to the United States*: *Hearing before the Subcomm. on Nat'l Sec., Homeland Def. and Foreign Operations of the H. Comm. on Oversight and Gov't Reform*, 112th Cong. 9 (2011) [hereinafter *Assessing the Immediate Threat*] (statement of Sean McGurk, Director of National Cybersecurity and Communications Integration Center); U.S. DEP'T DEF., *supra* note 240, at 8 (noting the Department of Defense's intent to partner with other government agencies). The reference to Homeland Security's responsibility for protecting *government* civilian networks seems to mean just that. *But see Assessing the Immediate Threat*, *supra* note 301 (noting that Homeland Security also "works with" private sector "owners and operators" of critical infrastructure components to "bolster their cybersecurity preparedness").

302. 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.*, *Mission and Responsibilities*, U.S. DEP'T HOMELAND SEC., http://ipv6.dhs.gov/xabout/responsibilities.shtm (last updated Feb. 22, 2012). A third reason is that the Department incorporates agencies that perform law enforcement functions. *See* DEP'T OF HOMELAND SEC., *supra* note 300, at 38–39 (containing DHS Organizational Chart).

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 Part 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.[303] 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.[304]

As matters currently stand, Cyber Command will have to utilize the attribution processes described in Part 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.[305] 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.[306]

General Alexander's primary problem, therefore, is that it may be impossible for the military to make such a determination for a cyber-attack quickly enough for a timely response be-

---

303. *See* 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); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1551–52 (2010).

304. *See supra* Part II.D.

305. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51(3), 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 (Protocol II), art. 13(3), June 8, 1977, 1125 U.N.T.S. 609.

306. *See, e.g.*, ALLAN W. KURKI, OPERATION MOONLIGHT SONATA: THE GERMAN RAID ON COVENTRY 71–80 (1995) (describing the Battle of Britain: "German air attacks carried out against Great Britain early in World War II"); Richard Goldstone, *The Trial of Saddam Hussein: What Kind of Court Should Prosecute Saddam Hussein and Others for Human Rights Abuses*, 27 FORDHAM INT'L L.J. 1490, 1502 (2004).

cause 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 categorically parsing threat response authority between them.[307] But as we saw earlier, General Alexander also confronts an institutional problem: fusing six distinct cyber commands into a coordinated, coherent cyber-response effort.[308] We will return to this issue in Part IV.

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

B. LAW ENFORCEMENT

As we saw in Part 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.[309] Some countries have a national penal code and a national police agency that enforces that code.[310] But because it is a federal state,[311] 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

---

307. It also arises from the fact that our definitions of war assume traditional, kinetic conflict. *See, e.g.*, U.N. Charter art. 51 (using the term "armed attack"); Definition of Aggression, G.A. Res. 3314 (XXIX), Article I, U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc. A/9631, at 142-143 (Dec. 14, 1974) (using the phrase "use of armed force"). The United States has made little, if any, progress toward reconciling the law of war and cyber-attacks. *See* 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.

308. *See supra* note 280 and accompanying text.

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

310. *See, e.g.*, Kuk Cho, *Korean Criminal Law: Moralist Prima Ratio for Social Control*, 1 J. KOREAN L. 77, 79–95 (2001) (describing the Korean Penal Code).

311. *See generally* Steven G. Calabresi & Nicholas Terrell, *The Number of States and the Economics of American Federalism*, 63 FLA. L. REV. 1, 2 (2011) (explaining that with fifty states, the United States is the largest federation in the world).

criminal codes (one for each state, one for the District of Columbia and a federal criminal code).[312] These codes require a corresponding, two-tiered law enforcement structure: one tier consists of the over 15,000 state and local agencies[313] that respectively enforce state criminal codes.[314] 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.[315]

The other tier is composed of agencies that enforce federal law. Five of them—the Federal Bureau of Investigation, the

---

312. 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.").

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. Ronald L. Gainer, *Federal Criminal Code Reform: Past and Present*, 2 BUFF. CRIM. L. REV. 45, 53 (1998); 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* 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, *2008 Criminal Tax Manual, Table of Contents*, http://www.justice.gov/tax/readingroom/2008ctm/CTM%20TOC.htm (last visited Oct. 8, 2012).

313. *See supra* note 3 (explaining that state and local law enforcement agencies employ an estimate of over 750,000 officers). State agencies, which are variously known as State Police, Highway Patrol or State Patrol, operate statewide. BRIAN A. REEVES, BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 233982, CENSUS OF STATE AND LOCAL LAW ENFORCEMENT AGENCIES 2008, at 6–7 (2011). Local law enforcement consists of county agencies, e.g., sheriff's or county police agencies, and municipal law enforcement agencies. *Id*.

314. For our purposes, "state law" includes both the laws adopted at the state level and any laws adopted by subdivisions of a state. S*ee*, *e.g.*, ALASKA STAT. § 18.65.080 (2010) (stating state troopers enforce "all criminal laws of the state"); COLO. REV. STAT. § 16-2.5-103(1) (2012) (stating sheriff's authority includes enforcing all laws of the state); NEV. REV. STAT. ANN. § 493.190 (Lexis-Nexis 2011) (municipal officers responsible for enforcing "state and municipal laws").

315. *See*, *e.g.*, DEL. CODE ANN. tit. 11, § 8302 (2007) (stating state police "primary law enforcement agency within the State"); WASH. REV. CODE ANN. § 36.28.010 (West 2003) (stating sheriff is "conservator of the peace of the county"); 42 PA. CONS. STAT. ANN. § 8951 (West 2007) (stating municipal officer has jurisdiction "within the territorial limits of a municipality").

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.[316] And because these agencies operate under the 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 U.S."[317] and, under certain circumstances, abroad.[318]

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.[319] This reduces, but does not eliminate, the potential for inter-agency conflicts.[320] Instances can and do arise in which, say, the State Po-

---

316. *See* CYBER-THREATS, *supra* note 7, at 152–53. *See also, e.g.*, 18 U.S.C. § 3052 (2006) (stating Federal Bureau of Investigation powers); 18 U.S.C. §§ 1029(d), 1030(d)(1), 3056 (2006) (stating Secret Service authority); 18 U.S.C. § 3051 (2006) (stating Bureau of Alcohol, Tobacco, Firearms and Explosives authority); Drug Abuse Prevention and Control Act, 21 U.S.C. § 878 (2006) (stating Drug Enforcement Administration authority); 19 U.S.C. § 1589a (2006), 22 C.F.R. § 127.4 (2012) (stating 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 (ICE)*, ALLGOV.COM, http://www.allgov.com/agency/U_S__Immigration_and_Customs_Enforcement_ICE. For examples of other agencies that play a less significant role in federal law enforcement, see BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, NCJ 212750, FEDERAL LAW ENFORCEMENT OFFICERS, 2004 at 2 (2006).

317. 18 U.S.C. § 7 (2006).

318. 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. 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.* at 1170–71; *see, e.g.*, 18 U.S.C. § 1030(e)(2)(b) (2006) (stating extraterritorial jurisdiction under the federal computer crime statute).

319. *See, e.g.*, DEL. CODE ANN. tit. 11, § 8302 (2007) (stating state police "primary law enforcement agency within the State"); WASH. REV. CODE ANN. § 36.28.010 (West 2003) (stating sheriff is "conservator of the peace of the county"); 42 PA. CONS. STAT. ANN. § 8951 (West 2007) (stating municipal officer has jurisdiction "within the territorial limits of a municipality").

320. Funding can be a source of conflict. *See, e.g.*, *Sheriffs: State Police Du-*

lice and the County Sheriff both have jurisdiction in a given matter,[321] which can create conflicts as to who should take the lead.[322] Over the last few years, state and local agencies have used multi-jurisdictional task forces to reduce, if not eliminate, such conflicts.[323]

Historically, the more serious conflicts arose between state and local agencies and their federal counterparts.[324] 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.[325]

That leaves the federal agencies, which have certainly not

---

plicate Our Efforts, DETROIT NEWS, September 7, 2005 at B1, *available at* 2005 WLNR 26971791.

321. 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. Garden City police, the Finney County Sheriff and the Kansas Highway Patrol would all have jurisdiction to investigate the crime. *Compare* DEL. CODE ANN. tit. 11, § 8302 (2007) (giving state-wide jurisdiction to state officers), *with* WASH. REV. CODE ANN. § 36.28.010 (West 2003) (giving county-wide jurisdiction to county officers), *and* 42 PA. CONS. STAT. ANN. § 8951 (West 2007) (giving jurisdiction within a municipality to municipal officers).

322. *See, e.g.,* Reid J. Epstein, *Suffolk Rejects Funds for Bomb Dog*, NEWSDAY, Dec. 23, 2010, at A15, *available at* 2010 WLNR 25275547. *See also* Joan Vennochi, Op-Ed., *Carson Beach: Whose Turf Is It?*, BOS. GLOBE, June 2, 2011, at A15; Vivian Yee*, Troopers Absent at City Turf Hearing*, BOS. GLOBE, June 29, 2011, at B1.

323. *See, e.g.*, Ron Jackson, *Task Force Sought for Pending Cases*, OKLAHOMAN, Dec. 2, 2009, at 7A, *available at* 2009 WLNR 24400863; Robert Medley & Michael Kimball, *3 City Residents Jailed in Crime Spree*, OKLAHOMAN, November 2, 2010, at 18A, *available at* 2010 WLNR 21967934. S*ee also* Anne C. Pogue, *If It Weren't for the Flip Side—Can the USA Patriot Act Help the U.S. Pursue Drug Dealers and Terrorists Overseas, Without Overstepping Constitutional Boundaries at Home?*, 14 CORNELL J.L. & PUB. POL'Y 477, 481 (2005) (indicating that the use of task forces dates back to the 1970s).

324. *See, e.g.*, Daniel Richman, *The Past, Present, and Future of Violent Crime Federalism*, 34 CRIME & JUST. 377, 405 (2006) (highlighting the conflict between local and federal enforcers in violent crime); David McLemore, *Interdiction Not Answer, Officers Say*, DALL. MORNING NEWS, Aug. 30, 1988, at 6A, *available at* 1988 WLNR 2258214 (noting the "continuing turf battles among federal and state law enforcement agencies"); *see also* Pierre Thomas, *Freeh Becomes Fifth Director of FBI*, WASH. POST, Sept. 2, 1993, at A6 (noting that the new director pledges to end "turf battles" among "federal, state and local law enforcement").

325. *See* Stephen D. Mastrofski & James J. Willis, *Police Organization Continuity and Change: Into the Twenty-First Century*, 39 CRIME & JUST. 55, 124 (2010); Robert M. Bloom & Hillary Massey, *Accounting for Federalism in State Courts: Exclusion of Evidence Obtained Lawfully by Federal Agents*, 79 U. COLO. L. REV. 381, 397 (2008). *But see* Dafna Linzer, *In New York, A Turf War in the Battle against Terrorism*, WASH. POST, Mar. 22, 2008, at A1, A4.

been immune to turf wars.[326] 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.[327] One reason why such conflicts persist among federal agencies is that, unlike their state and local counterparts, federal agencies' jurisdictional authority is predicated not on geographical turf, but on what a recent report refers to as "operational turf."[328]

In situations like the hypothetical noted earlier,[329] in which a crime scene falls within the State Police's and the local Sheriff's geographical turf, the State Police may 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,[330] but this is a matter of operational efficiency and, as such, does not define the legitimate scope of an agency's operations.[331] That is a function of "operational turf," that is, of the statutes that define a given agency's investigative authority.[332]

If these statutes parsed investigative authority out among the five agencies listed above in a fashion analogous to how

---

326. *See, e.g.*, *Prepared Statement of Senator Chuck Grassley of Iowa*, GRASSLEY.SENATE (Nov. 18, 2009), http://www.grassley.senate.gov/news/Article.cfm?customel_dataPageID_1502=24164; Joe Davidson, *Drug Cartels Corrupting U.S. Law Enforcement*, WASH. POST, June 9, 2011, at B4.

327. *See*, *e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-314, LAW ENFORCEMENT COORDINATION: DOJ COULD IMPROVE ITS PROCESS FOR IDENTIFYING DISAGREEMENTS AMONG AGENTS 8 (2011) (noting one-third of agents surveyed "reported experiencing disagreements over the past 5 years with another DOJ component when determining roles and responsibilities during an investigation."). For more on the evolution and current state of federal agency conflicts, see KIRSTIN M. FINKLEA, CONG. RESEARCH SERV., R41927, THE INTERPLAY OF BORDERS, TURF, CYBERSPACE, AND JURISDICTION: ISSUES CONFRONTING U.S. LAW ENFORCEMENT 19–25 (2012).

328. FINKLEA, *supra* note 327, at 21.

329. *See supra* note 321.

330. *See*, *e.g.*, FBI, TODAY'S FBI 2010–2011 at 5 (2007), *available at* http://www.fbi.gov/stats-services/publications/facts-and-figures-2010-2011/facts-and-figures-2010-2011-pdf.

331. FBI, THE FBI: A CENTENNIAL HISTORY 1908–2008 at 108 (2008).

332. *See* FINKLEA, *supra* note 327, at 21–23.

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.[333] 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.[334] Criminals' increasing use of cyberspace is only exacerbating the difficulties federal agents already face.[335]

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:[336] 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 purely personal.[337] An attack on a financial institution might be a cybercrime committed by a greedy United States citizen "in" the United States, but it might, instead, be (i) a cybercrime committed by a non-United States citizen operating from abroad or (ii) a cyber-sortie carried out by a hostile nation-state's own cyber command.[338]

---

333. *Id.* at 21; *see also, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 327, at 1 ("[I]n 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.").

334. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 327, at 8.

335. *See* FINKLEA, *supra* note 327, at 18; U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-876T, INFORMATION SECURITY: CYBER THREATS FACIILITATE ABILITY TO COMMIT ECONOMIC ESPIONAGE 3–6, 10–12 (2012). *See also supra* II.D.

336. *See supra* Part III.A.2.

337. *See supra* Part II.B.

338. *See, e.g.,* John Leyden, *Leaked U.S. Cables Finger Chinese Army Hackers for Cyber-Spying*, REGISTER (Apr. 18, 2011, 14:15 GMT), 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,

If the attack hypothesized above constitutes domestic cybercrime committed by a United States citizen, it clearly falls within United States law enforcement's investigative authority under the bifurcated approach outlined above.[339] 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,[340] but it is still their default responsibility.[341]

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.[342] 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.[343] As we also saw, those markers do not (necessarily) exist in cyberspace: bits and bytes do not arrive bearing national insignia nor do they constitute weaponry that only nation-states can employ.[344] The bits and bytes used to launch a cyberwar attack of the type we are hypothesizing would begin their voyage to their United States target from a location outside the territorial United States, but as we have seen,[345] that

---

which would presumably be within law enforcement's investigative authority. *At Light Speed*, *supra* note 31, at 423; Michael J. Robbat, Note, *Resolving the Legal Issues Involving the Use of Information Warfare in the International Forum*, 6 B.U. J. SCI. & TECH. L. 264, 287 (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, 398–401 (2006) (noting the long list of "usual suspects" for internet economic espionage).

339. *See supra* Part II.A–B.

340. *See generally* 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) (discussing two high-profile cybercrime cases where the FBI had to overcome legal and procedural hurdles to gather international evidence).

341. *See supra* Part II.A–B.

342. *See supra* Part II.B–C.

343. *See supra* Part II.B–C. As we saw earlier, one of the markers is that the attack is directed at a military target. For example, the 1941 attack that brought the United States into World War II was directed at Pearl Harbor, a U.S. naval base. *World War II: Pearl Harbor*, ATLANTIC (July 31, 2011), http://www.theatlantic.com/infocus/2011/07/world-war-ii-pearl-harbor/100117.

344. *See supra* Part II.B.

345. *See supra* Part II.A–B.

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 United States territory, it would be quite reasonable for United States law enforcement officers to assume an attack is crime, rather than war.[346] 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.[347] The United States military has for decades monitored geographical vectors (i.e., United States 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.[348] 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.[349]

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,[350] 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.[351] If a state were to do this (and for all we know, one already has),[352] United States law enforcement officers would

---

346. Aside from anything else, the fact that the attack targets a civilian entity inferentially suggests it is crime, not war. *See id.*

347. *See id.*

348. Aliya Sternstein, *Congress, Administration Grapple with Cyber Defense Authority*, NEXTGOV (Apr. 11, 2011), http://www.nextgov.com/cybersecurity/2011/04/congress-administration-grapple-with-cyber-defense-authority/48873 (noting that General Alexander confirms that the U.S. Cyber Command cannot monitor civilian networks).

349. *See supra* Part II.B.

350. 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*, DEFENSE TECH (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, *IMF Cyber-Attack Led by Hackers Seeking 'Privileged Information,'* GUARDIAN (June 13, 2011), http://www.guardian.co.uk/business/2011/jun/12/imf-cyber-attack-hack ("[cyberwar] waged by governments for economic . . . purposes.").

351. *See supra* Part II.B. Estonia may have been the target of a similar attack in 2007. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 205–06 (2009).

352. *See* Arthur, *supra* note 350 (describing various attacks on U.S. com-

construe the attacks as cybercrime and do their best to respond, presumably after the fact.[353] If the response came after the attacks ended, then they would have inflicted the intended damage and the United States officers would be left with the essentially futile task of trying to track down and apprehend the perpetrators.[354] 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.[355]

All of this has serious implications for the country's security: the United States military has been, and is, responsible for protecting the nation 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 reliably attributed to a hostile nation-state and/or (ii) only involve the use of cyberspace.[356]

---

panies potentially made by foreign states).

353. *See supra* note 224. 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 hypothetical 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.

354. Scott Charney, *The Internet, Law Enforcement and Security*, *in* 2 FIFTH ANN. INTERNET LAW INSTITUTE 937, 945 (Practising Law Inst. ed., 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.").

355. *See, e.g.*, ENEKEN TIKK ET AL., COOP. CYBER DEF. CTR. OF EXCELLENCE, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 75 (2010), *available at* http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (explaining that 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").

356. *See, e.g.*, U.N. Charter, *supra* note 307, at art. 51; *see also* Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 A.F. L. REV. 121, 144–48 (2009) (noting that cyber-attacks do not

This leaves law enforcement, which has historically responded to internal attacks involving citizen-on-citizen victimization.[357] As we saw above,[358] United States law enforcement now finds it increasingly necessary to respond to external attacks that involve the online victimization of United States citizens by noncitizens. Since these attacks involve individual-on-individual victimization and since the perpetrators' motives and the "harms" they inflict fall within existing principles of criminal liability, the investigation of the attacks clearly fits within United States law enforcement's investigative authority.[359]

As a practical matter, United States law enforcement officers cannot effectively investigate all or even a substantial portion of the transnational cybercrime attacks that target United States 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 United States 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.[360] There are processes by which United States law enforcement officers can obtain evidence from abroad, but they are complex, uncertain and move at a glacial pace.[361] 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.[362] 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.[363]

---

qualify as acts of war under current laws of warfare).

357. *See supra* Part II.A.

358. *See supra* Part II.B.

359. *See supra* Part II.B.

360. *See, e.g.,* CYBER-THREATS, *supra* note 7, at 201–22.

361. *See* SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 142–48 (2010).

362. *Criminal Law for Cyberspace*, *supra* note 7, at 80.

363. McAfee's 2011 report outing of "Operation Shady Rat," a five-year series of cyber-attacks on corporate and government targets, illustrates how difficult it can be to determine whether an attack is mere cybercrime or some-

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.[364]

And while the military's mission specifically encompasses extraterritorial threat response, we cannot, as noted above,[365] 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 cyber-attacks targeting the U.S. and/or to apprehend the perpetrator(s) of such attacks, that would constitute an act of war, though the cyber-attacks themselves would not.[366]

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

---

thing more. *Compare* Jim Finkle, *"State Actor" Behind Slew of Cyber Attacks*, REUTERS (Aug. 3, 2011, 7:17 PM), http://www.reuters.com/article/2011/08/03/us-cyber-attacks-idUSTRE7720HU20110803?feedType=RSS&feedName=topNews&rpc=71, *with* Gabriel Perna, *McAfee's Rivals Scoff at Shady RAT Report*, FIN. CONTENT (Aug. 5, 2011, 16:41 PM), http://markets.financialcontent.com/stocks/news/read/19167626/McAfee%e2%80%99s_Rivals_Scoff_at_Shady_RAT_Report.

364. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (1987) ("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.* §§ 432 cmt. B, 433; U.S. DEPT. OF JUSTICE, CRIMINAL RESOURCE MANUAL § 267 (1997), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00267.htm (noting the sovereignty issues that arise when gathering evidence abroad).

365. *See supra* note 356 and accompanying text.

366. *See supra* note 307 and accompanying text.

next subpart.

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 cyber-attacks were introduced in Congress.[367] One of them—the Protecting Cyberspace as a National Asset Act of 2010 ("Protecting Cyberspace")—was introduced by Senators Lieberman, Collins, and Carper.[368] 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."[369] Among other things, it created 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."[370]

The Protecting Cyberspace bill included what became controversial provisions concerning private sector entities that were part of the nation's "critical infrastructure."[371] The NCCC

---

367. *See* Elizabeth Montalbano, *Senate Bill Proposes Office of Cyberspace Policy*, INFO. WK. (June 14, 2010, 8:00 AM), http://www.informationweek.com/government/security/senate-bill-proposes-office-of-cyberspac/225600464 (noting Lieberman-Collins-Carper, Kerry, and Rockefeller-Snowe bills in the Senate, Lipinski bill in the House).

368. *See* Emelie Rutherford, *Senate Committee Oks Cybersecurity Bill on Majority Leader's Radar*, DEF. DAILY, June 25, 2010, *available at* 2010 WLNR 14036808.

369. *Lieberman, Collins, Carper Unveil Major Cybersecurity Bill to Modernize, Strengthen, and Coordinate Cyber Defenses,* U.S. SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFF. (June 10, 2010), http://www.hsgac.senate.gov/media/majority-media/lieberman-collins-carper-unveil-major-cybersecurity-bill-to-modernize-strengthen-and-coordinate-cyber-defenses (quoting Senator Collins).

370. Protecting Cyberspace as a National Asset Act of 2010, S. 3480, 111th Cong. § 242(f)(1)(A) (noting this is as introduced in the Senate).

371. *See id.* § 248. The bill incorporated the definition of critical infrastruc-

Director was required, "on a continuous . . . basis, [to] identify and evaluate the cyber vulnerabilities to covered critical infrastructure."[372] 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.[373]

The Protecting Cyberspace bill made the NCCC Director responsible for ensuring that the "owners and operators of critical infrastructure" developed plans for responding to a "national cyber emergency."[374] The bill also authorized the President to declare such an emergency.[375] If a President declared a national cyber emergency, the owners and operators of critical infrastructure components were then required to implement their required response plans and the NCCC Director was to "develop and coordinate emergency measures or actions necessary to preserve the reliable operation . . . of covered critical infrastructure."[376]

The 2010 Lieberman-Collins-Carper legislation so 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 de-

---

ture contained in the USA PATRIOT Act, 42 U.S.C. § 5195c(e) (2006). *Id.* § 3(2). 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." 42 U.S.C. § 5195c(e) (2006).

372. S. 3480 § 248(a)(1).

373. *Id.* § 248(b)(1).

374. *Id.* § 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 vulnerability in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure." *Id.* § 241(17). National information infrastructure is defined as information infrastructure that is "owned, operated, or controlled within or from the United States; or if located outside the United States, the disruption of which could result in national or regional catastrophic damage in the United States; and that is not owned, operated, controlled, or licensed for use by a Federal agency." *Id* § 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.* § 241(10).

375. *Id.* § 249(a)(1).

376. *Id.* § 249(a)(3)(A)–(B).

veloped and implemented the security measures and response plans required by the Protecting Cyberspace bill.[377] 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.[378] The Director was also authorized to evaluate the security measures and response plans submitted by those responsible for critical infrastructure components.[379]

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."[380] 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.[381] Section 2(c) of the 2011 bill said 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."[382] 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.[383]

On February 14, 2012, Lieberman, along with Senators Susan Collins, Diane Feinstein, Jay Rockefeller, and Sheldon Whitehouse, introduced the next iteration of his proposed cybersecurity legislation: S. 2105—the Cybersecurity Act of

---

377. *Id.* § 250(a)(1).

378. *Id.* § 250(a)(2), (c)(1).

379. *Id.* § 250(b).

380. Declan McCullagh, *Senators Propose Granting President Emergency Internet Power*, CNET (June 10, 2010, 8:25 PM), http://news.cnet.com/8301-13578_3-20007418-38.html (quoting the Center for Democracy and Technology).

381. Declan McCullagh, *Internet "Kill Switch" Bill Gets a Makeover*, CNET (Feb. 18, 2011), http://news.cnet.com/8301-31921_3-20033717-281.html.

382. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 2(c) (2011).

383. McCullagh, *supra* note 381. 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. S. 3480; S. 413.

2012.[384] Like its predecessors, S. 2105 made the Department of Homeland Security primarily responsible for (i) identifying and assessing "cyber risks" to critical infrastructure components, (ii) working with the owners and operators of the various critical infrastructure components to develop "risk-based cybersecurity performance requirements" for those components, and (iii) implementing those requirements.[385] And like its predecessors, S. 2105 let entities that designated as critical infrastructure components subject to the Act's requirements challenge that designation in a civil action brought exclusively in the U.S. District Court for the District of Columbia.[386]

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.[387]

---

384. *See Cybersecurity Act of 2012 (Proposed)*, COUNCIL ON FOREIGN REL. (Feb. 2012), http://rebecca.cfr.org/cybersecurity/cybersecurity-act-2012-proposed/p27479; Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012) (introduced in the Senate on Feb. 14, 2012).

On July 19, 2012, Senator Lieberman introduced S. 3414, a replacement bill—the Cybersecurity Act of 2012 (CSA2012). Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012) (introduced in the Senate on July 19, 2012). Like its predecessors, the bill was lengthy (211 pages) and covered much of the same ground. *See id.* The new bill was applauded by privacy advocates, who noted that it included provisions ensuring that the legislation did not undermine First Amendment protections of free speech, ensuring that only civilian agencies (versus the National Security Agency) were in charge of cybersecurity efforts, and ensuring that data would not be shared with law enforcement except in specific, limited circumstances. *See* Rainey Reitman & Lee Tien, *New Cybersecurity Proposal Patches Serious Privacy Vulnerabilities*, ELECTRONIC FRONTIER FOUND. (July 19, 2012), https://www.eff.org/deeplinks/2012/07/new-cybersecurity-proposal-patches-serious-privacy-vulnerabilities.

The new bill did not survive, however: on August 2, 2012, the CSA2012 "fell eight votes shy" of cloture in the Senate. Gerry Smith, *Cyber Security Law Fails to Pass Senate Before Month-Long Break*, HUFFINGTON POST (Aug. 3, 2012, 11:55 AM), http://www.huffingtonpost.com/2012/08/02/cyber-security-law_n_1733751.html; *see also* Ed O'Keefe & Ellen Nakashima, *Cybersecurity Bill Fails in Senate,* WASH. POST, Aug. 3, 2012, at A3. Some applauded its demise. *See, e.g.*, Jody Westby, *Congress Needs to Go Back to School on Cyber Legislation*, FORBES (Aug. 13, 2012, 9:34 PM), http://www.forbes.com/sites/jodywestby/2012/08/13/congress-needs-to-go-back-to-school-on-cyber-legislation ("The Lieberman/Collins bill was a masterful piece of deception that was intended to bamboozle businesses into believing that the legislation was not a massive extension of regulatory authority.").

385. *See* S. 2105 §§ 2, 101–106.

386. *See id.* at § 103(c); *see also* S. 413 § 254(c)(2).

387. *See* Legislative Language: Law Enforcement Provisions Related to Computer Security, Enclosure to Letter from Jacob J. Lew, Dir., Exec. Office of

The primary difference between the proposals is that the White House plan 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 information infrastructure."[388]

---

the President: Office of Mgmt. & Budget, to John Boehner, Speaker of the House of Representatives and Joseph R. Biden, President of the Senate (May 12, 2011) [hereinafter White House, Cybersecurity Proposal], *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf; *see also* Letter from Jacob J. Lew, Dir., Exec. Office of the President: Office of Mgmt. & Budget, to John Boehner, Speaker of the House of Representatives and Joseph R. Biden, President of the Senate (May 12, 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Cybersecurity-letters-to-congress-house-signed.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* White House, Cybersecurity Proposal, *supra* note 387.

388. *See* White House, Cybersecurity Proposal, *supra* note 387, § 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.* §§ 2–5, 8. This portion of the White House plan uses the same definition of critical infrastructure as the legislation proposed by the Senators. *Compare id.* § 10(3), *with supra* note 371.

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* White House, Cybersecurity Proposal, *supra* note 387, § 243(c)(5).

In the wake of the CSA2012's failure in the Senate, one of its sponsors, Senator Dianne Feinstein, urged President Obama to "use your full authority to protect the U.S. economy and the networks we depend on from future cyber attack." Press Release, U.S. Senator Dianne Feinstein, *Feinstein Calls on Obama to Protect Computer Networks from Cyber Attacks*, (Aug. 28, 2012), http://www.feinstein.senate.gov/public/index.cfm/2012/8/feinstein-calls-on-president-to-protect-critical-infrastructure-from-cyber-attacks. Feinstein noted that while "an Executive Order cannot convey protection from liability that private sector companies may face," the President and his administration could issue "cybersecurity standards and provide technical assistance to companies willing to take voluntary steps to improve their security." *Id.*

Feinstein's letter, plus a provision in the 2012 Democratic National Platform, caused concern among some that the Administration might resort to executive orders as a way to implement cybersecurity measures. *See, e.g.*, Jody Westby, *Businesses Beware: Heavy-Handed Tactics Planned for Cybersecurity*, FORBES (Sept. 7, 2012), http://www.forbes.com/sites/jodywestby/2012/09/07/

These were not the only proposals Washington has generated in the last three years; several bills have been proposed in the House of Representatives and either have been met with varying receptions or are still pending.[389] In July of 2011, Senator McCain, who wanted 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."[390] Senators Lieberman

---

businesses-beware-heavy-handed-tactics-planned-for-cybersecurity/. *See also* DEMOCRATIC NAT'L COMM., 2012 DEMOCRATIC NATIONAL PLATFORM 24 (2012), *available at* http://assets.dstatic.org/dnc-platform/2012-National-Platform.pdf ("[T]he President will continue to take executive action to strengthen and update our cyber defenses."). On September 6, 2012, one source reported that the "White House [was] circulating a draft of an executive order aimed at protecting the country from cyber-attacks" in the absence of legislative measures. Jennifer Martinez, *White House Circulating Draft of Executive Order on Cybersecurity*, HILL (Sept. 6, 2012), http://thehill.com/blogs/hillicon-valley/technology/248079-white-house-circulating-draft-of-executive-order-on-cybersecurity.

The 2012 Republican Party National Platform also criticized the Obama Administration's cybersecurity efforts:

> The current Administration's laws and policies undermine what should be a collaborative relationship and put both the government and private entities at a severe disadvantage in proactively identifying potential cyber-threats. The costly and heavy-handed regulatory approach by the current Administration will increase the size and cost of the federal bureaucracy and harm innovation in cybersecurity . . . .

REPUBLICAN NAT'L COMM., 2012 REPUBLICAN PLATFORM 41 (2012), *available at* http://www.gop.com/wp-content/uploads/2012/08/2012GOPPlatform.pdf.

389. *See, e.g.*, Brendan Sasso, *House to Vote on Four Cyber Bills, Leaves Out Lungren Measure*, HILL (Apr. 20, 2012), http://thehill.com/blogs/hillicon-valley/technology/222833-house-to-vote-on-four-cyber-bills-leaves-out-lungren-measure; Nicole Blake Johnson, *House Committees Approve 2 Cybersecurity Bills*, FED. TIMES (Apr. 18, 2012), http://www.federaltimes.com/article/20120418/CONGRESS01/204180305/100; *see also* Cybersecurity Enhancement Act of 2012, H.R. 2096, 112th Cong. (2012). Representative Michael Rogers introduced the Cyber Intelligence Sharing and Protection Act. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. (as introduced in House, Nov. 30, 2011). It passed the House of Representatives on April 26, 2012, but so far has not received any action in the Senate. *H.R. 3523: Cyber Intelligence Sharing and Protection Act*, GOVTRACK, http://www.govtrack.us/congress/bills/112/hr3523 (last visited Oct. 19, 2012). The bill has caused controversy because it allows Internet service providers to share information with the government and each other. *See, e.g.*, David Kravets, *House Passes Controversial Cybersecurity Measure CISPA*, WIRED.COM (Apr. 26, 2012), http://www.wired.com/threatlevel/2012/04/house-passes-cispa.

390. Ben Pershing, *On Cybersecurity, a Turf Battle*, WASH. POST, July 18,

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.[391] One commentator put the bickering, and the proliferation of cybersecurity committees and task forces, down to the fact that "lawmakers hate giving up turf."[392]

Aside from establishing that turf battles are not confined to federal and state agencies, the debate over McCain's proposed committee demonstrated that lawmakers and law enforc-

---

2011, at A11 (quoting Senator McCain). McCain pointed out that "the White House and the Energy, Commerce and Defense departments have all put forward separate initiatives on the subject" and argued that his proposed Select Committee on Cyber Security and Electronic Leaks would "quell" the competition "for cyber jurisdiction" that had arisen among Congressional committees. Marcus Weisgerber, *U.S. Senate Debates Cyber Oversight Proposal*, DEF. NEWS (July 19, 2011), http://www.defensenews.com/story.php?i=7135581&c=POL&s=TOP. 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* Press Release, Speaker of the House John Boehner, Speaker Boehner & Leader Cantor Announce New Cybersecurity Task Force Led By Rep. Thornberry (June 23, 2011), *available at* http://www.speaker.gov/News/DocumentSingle.aspx?DocumentID=248724. Also, Senator Harry Reid earlier introduced a bill that was designed to protect the U.S. from cyber-attack. *See* Cyber Security and American Cyber Competitiveness Act of 2011, S. 21, 112th Cong. (2011). And, in March of 2011, Congressman Jim Langevin introduced a bill to "significantly strengthen protections against dangerous cyber threats." Press Release, U.S. Congressman Jim Langevin, Langevin Introduces Bill to Strengthen Cybersecurity, Prevent Attacks (Mar. 16, 2011), *available at* http://langevin.house.gov/press-release/langevin-introduces-bill-strengthen-cybersecurity-prevent-attacks.

For the Department of Energy's legislative cybersecurity efforts, see *Cyber Security: Hearing Before the S. Comm. on Energy and Natural Resources*, 112th Cong. 7 (2011) (statement of Patricia Hoffman, Assistant Secretary, Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy). For the report of the Department of Commerce's task force on cybersecurity, see DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY (2011), *available at* 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 Part III.A.

391. Pershing, *supra* note 390 (quoting Senators Lieberman and Collins).

392. *Id.* In March of 2012, Senators McCain, Kay Bailey Hutchinson and "other Republicans" introduced the "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology (SECURE IT) Act." Brenda Sasso, *SECURE IT Act Introduced in the House,* HILL (Mar. 27, 2012), http://thehill.com/blogs/hillicon-valley/technology/218421-secure-it-act-introduced-in-the-house; *see also* Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012, S. 2151, 112th Cong. (2012).

ers 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.[393] Congress has acted with similar expedition on the other occasions when it was called upon to approve a military response to an external threat.[394]

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. Cyber-attacks 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.[395] 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 U.S. can no longer rely on natural barriers or man-made barriers such as NORAD[396] to detect and deflect cyber-attacks 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.

Cyber-attacks are pervasive for a related reason, i.e., they do not (necessarily) differentiate between "sovereign" targets

---

393. *See* Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No.107–243, 116 Stat. 1498 (2002).

394. *See* Declaration of State of War With Japan, S.J. Res. 116, 77th Cong. (1941).

395. *See*, *e.g.*, Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR, Apr. 2011, at 220, 234 (noting the widespread nature of attacks such as Operation Shady Rat).

396. *See* N. AM. AEROSPACE DEF. COMMAND, http://www.norad.mil (last visited Nov. 7, 2012).

and "citizen" targets.[397] Cybercriminals attack individuals, private sector entities and governmental and military targets, and the same is, or is likely to be, true of cyberterrorists.[398] Conversely, it is already apparent that "civilians," as well as "sovereigns," will be the targets of cyberwarfare.[399] 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.[400]

Finally, cyber-attacks 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).[401] This, as we saw above, further erodes the viability of the bifurcated approach,[402] all of which is why Congress, the White House, and various government agencies want to bring civilians into the cyber-threat response process.[403]

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 Part and in Part IV, primarily focuses on the conceptual issues.[404]

---

397. *See supra* Part II.B.

398. *See supra* Part II.B.

399. *See supra* Part II.B.

400. *See supra* Part II.B.

401. *See supra* Part II.B.

402. *See supra* Part II.B.

403. *See supra* Part II.B. For more on why private sector involvement is essential for the United States' ability to protect itself from cyber-threats, see Brenner & Clarke, *supra* note 40, at 1024–39.

404. 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.

2. Conceptual Issues

It is clear from the proposals outlined above that the U.S. 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 Part and take up management in Part 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, "some private sector stakeholders have expressed concern that increased federal intervention in private cyber networks would impose excessive burdens and . . . stifle innovation and commerce."[405] Companies also fear that government-imposed cybersecurity standards and practices could "have adverse effects on the private sector's ability to parry cyber-attacks."[406] And some say "asking private industry to deal with cybersecurity [i]s like having the airlines deal with air attacks."[407]

The first two concerns seem to reflect businesses' normal reservations about excessive government regulation.[408] As such, they go less to the legitimacy of the recruitment process

---

405. Richard Weitz, *Preventing the Next Private Sector Cyber Security Breach*, SECOND LINE DEF. (July 18, 2011), http://www.sldinfo.com/preventing-the-next-private-sector-cyber-security-breach. For similar views, see Letter from Cisco Systems, IBM and the Oracle Corporation, to U.S. Senators Lieberman and Collins (June 24, 2010), *available at* http://www.scribd.com/doc/34006241/Cisco-IBM-Oracle-letter-re-S-3480-06-24-10.

406. Weitz, *supra* note 405.

407. John Eggerton, *WH Cybersecurity Coordinator: Privacy, Speech Protections Are Core Tenets*, BROADCASTING & CABLE (Aug. 4, 2011, 10:03 AM), http://www.broadcastingcable.com/article/471972-WH_Cybersecurity_Coordinator_Privacy_Speech_Protections_Are_Core_Tenets.php.

408. *See, e.g.*, COMM. ON CAPITAL MKTS. REGULATION, INTERIM REPORT OF THE COMMITTEE ON CAPITAL MARKETS REGULATION at ix-xii (2006) (discussing regulatory costs on the private sector and its impact on financial markets), *available at* http://www.capmktsreg.org/pdfs/11.30Committee_Interim_Report REV2.pdf; Orion Corp. v. State, 747 P.2d 1062, 1076–77 (Wash. 1987).

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.[409] If such an effort focused only on cyberwar, their status would shift from noncombatant to combatant;[410] if it focused only on cybercrime and cyberterrorism, their status would shift from civilian to police officer.[411] In a blended cyberwar/crime/terrorism response effort, the shift is more generic. Civilians transform from nonparticipants into participants, 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.[412] 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.[413] As far as I can tell, neither of the bills nor the White House proposal explains what such a "response" entails.[414] It would certainly involve defensive measures, i.e., efforts to secure systems and withstand the ef-

---

409. *See* Brenner & Clarke, *supra* note 40, at 1024–39.

410. *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).

411. *See Criminal Law for Cyberspace*, *supra* note 7, at 60–64 (development of police forces eliminated "citizen involvement" in crime/terrorism control and gave that task to professional law enforcement officers).

412. Brenner & Clarke, *supra* note 40, at 1048.

413. *See supra* notes 374–376, 383 and accompanying text. *See also* Cybersecurity and Internet Freedom Act of 2011, S. 413, 122th Cong. §§ 248(b)(3), 249(a)(3)(A) (2011); White House, Cybersecurity Proposal, *supra* note 387, §§ 243(c)(5)(B), 243(c)(9)–(10).

414. This is perhaps not surprising, given that in August of 2011 the Government Accountability Office "told Pentagon officials to define 'cybersecurity' so the military services adopt the same terminology." Aliya Sternstein, *Auditors: Pentagon Budget Has Fuzzy Numbers*, NEXTGOV (Aug. 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 (explaining that the GAO criticized the Department of Defense for not having "uniformly defined" what "constitutes a cyberforce").

fects 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.[415]

One could argue that participating in a purely defensive response is not enough to transform a civilian entity from cyber-noncombatant to cyber-combatant,[416] 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 cyber-attacks. 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 cyber-field of battle on which United States forces could confront, and defeat, an ascertainable unified opponent. As we saw earlier, that

---

415. *See, e.g.*, U.S. SEC'Y OF THE AIR FORCE, AIR FORCE INSTRUCTION NO. 51-402, LEGAL REVIEWS OF WEAPONS AND CYBER CAPABILITIES 5 (2011), *available at* 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*, GOV'T EXECUTIVE (Aug. 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 Department of Defense has indicated that damage to United States critical infrastructure or injury to United States citizens can warrant the use of kinetic force in response. *See* Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1.

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*, MCAFEE SECURITY J. (McAfee, Santa Clara, Ca.), Issue 6, 2010, at 3–4, 5–8, 27–30, *available at* 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, 174–78 (2005) (discussing a virus security technology developed by Symbiot that launches "'counterstrikes' against digital intruders").

416. *Cf.* Brenner & Clarke, *supra* note 40, at 1026–35.

scenario, while not impossible, is unlikely.[417]

I also find this scenario problematic for another reason: I do not see how Cyber Command and its constituent cyber commands could possibly "defend" United States 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;[418] 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.[419] But even if Cyber Command satisfactorily addresses these and other operational issues, I do not see how it, alone, could "defend" United States civilians from cyber-attackers. As I noted above, cyber-threats, unlike their real-space counterparts, are insidious, pervasive, and enigmatic which means a cyber-attack 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.[420] 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 United States 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)

---

417. *See supra* Part II.B.

418. *See, e.g.*, J. Nicholas Hoover, *Senate Confirms Military Cybersecurity Chief*, INFO. WK. (May 11, 2010, 12:48 PM), http://www.informationweek.com/news/government/security/224701513 (noting that some "details of Cyber Command remain to be worked out, such as force size").

419. *See supra* note 275 and accompanying text; *see also supra* note 414.

420. 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* RAOUL NAROLL ET AL., MILITARY DETERRENCE IN HISTORY 3–4 (1974).

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 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 from the employees who were in charge of those systems?[421] I suspect the answer will, at least in part, depend on the nature and circumstances of the attack.[422]

My point is that I do not believe United States companies will be able to rely solely on defensive measures in the event of a cyber-attack. 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 United States 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 private 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 United States 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 offen-

---

421. 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).

422. 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 How a "Denial of Service" Attack Works*, CNET NEWS (Feb. 9, 2000), http://news.cnet.com/2100-1017-236728.html. 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* Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, at 152, 155 ("Stick a flash drive with the virus into a laptop and it enters the machine surreptitiously . . .").

sive, as well as defensive, measures. The person who analogized "asking private industry to deal with cybersecurity" to "having the airlines deal with air attacks"[423] clearly recognized that this is an implicit element of the current cybersecurity proposals. It is not surprising that that commentator 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).[424] In the preceding centuries, civilians bore most, if not all, of the responsibility for ensuring their societies were protected from both internal and external threats.[425] We have forgotten that; we assume security is a matter that is to be, and will be, dealt with by the appropriate professionals.[426]

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.[427] If nothing else, this is evident from how Howard Schmidt, the White House's "Cyber Czar,"[428] responded to the air-attack/cyber-attack analogy: He indicated that "building security into systems has become a

---

423. *See supra* note 407 and accompanying text.

424. *See Criminal Law for Cyberspace*, *supra* note 7, at 60–65. *See also* CYBER-THREATS, *supra* note 7, at 15–16, 165–69, 213–15; Brenner & Clarke, *supra* note 40, at 1073–75.

425. *See Criminal Law for Cyberspace*, *supra* note 7, at 60–65; CYBER-THREATS, *supra* note 7, at 15–16, 165–69, 213–15.

426. *See Criminal Law for Cyberspace*, *supra* note 7, 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.*, State v. Emmons, 161 P.3d 920, 926 (N.M. Ct. App. 2007); Staben v. Hernandez, No. 06cv1407-IEG(BLM), 2007 WL 2238657 at *1, *5–11 (S.D. Cal. 2007). And as noted earlier, if a civilian engages in military combat, his or her status changes from noncombatant to unlawful combatant. *See supra* notes 227 and 410.

427. *See, e.g.*, 157 CONG. REC. S909, S911 (daily ed. Feb. 17, 2011) (statement of Sen. Collins) (noting that the "private sector is also under attack" in cyberspace). Additionally, note, "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." *Id.*

428. *See* Andy Greenberg, *Finally, A Cyber Czar*, FORBES (Dec. 21, 2009), http://www.forbes.com/2009/12/21/cyber-czar-named-security-business-in-the-beltway-schmidt.html.

business imperative," and he noted that the government needs to "help" those who do not realize this to "understand they have that shared responsibility."[429] Schmidt might more accurately have said that the 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.[430] And law enforcement agencies hire officers from candidates who voluntarily apply for those positions.[431] 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 or military combat on the quite logical premise that untrained civilians are only likely to impede trained professionals in the performance of their duties.[432] In

---

429. Eggerton, *supra* note 407. 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 cyber-attack scenarios. *See Cyber Storm: Securing Cyberspace*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/files/training/gc_1204738275985.shtm (last visited Dec. 31, 2012).

430. *See* Tim Donahue, Note, *The Constitutionality of Stop-Loss and Why It Is Better for the Country Than the Draft*, 44 NEW ENG. L. REV. 71, 78–83 (2009).

431. *See, e.g.*, *Police Recruitment and Retention Clearinghouse*, RAND, http://www.rand.org/ise/centers/quality_policing/cops.html (last visited Nov. 7, 2012).

432. *See, e.g.*, Williams v. Tharp, 914 N.E.2d 756, 765 (Ind. 2009) (reasoning that it is best to leave the task of investigating potential criminal activity and "deciding upon the appropriate response to trained professionals"); *see also supra* note 426.

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."

Gross, *supra* note 395, at 225. This article also suggests that at least some of

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 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, or their assets, from cyber-threats while, at the same time, maintaining civilian confidence in the government's ability to protect them from other threats.[433]

There is another downside for 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.[434] The entities would have to 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

---

the U.S. corporate sector's disinclination to take responsibility for cybersecurity is the result of companies not sharing information about the cyber-attacks they have sustained. *See id.* at 234 ("[T]op corporate managers—following the advice of their lawyers—are reflexively keeping breach information secret from other companies that are trying to defend themselves.").

433. 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 . . . ."

Gross, *supra* note 395, at 234. I suspect we will see the disinclination eroded gradually, as news outlets and other media publicize leaked information about cyber-attacks and, in so doing, begin to cultivate attitudes similar to those that have driven many citizens to invest in alarm systems and burglar bars.

434. *See supra* notes 374–379, 383, 388 and accompanying text.

review by the official who is assigned responsibility for implementing this part of the proposed cybersecurity initiative.[435]

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.[436] This 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 Part 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].[437]

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

---

435. *See, e.g.*, Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 250(a)–(b) (2011).

436. 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 (Jan. 25, 2010), http://www.csoonline.com/article/518764/companies-on-it-security-spending-where-s-the-roi. An article on cyberwar 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 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.

Gross, *supra* note 395, at 233.

437. *Id.* at 234 (quoting General Michael Hayden, former director of the NSA and of the CIA).

it might best be achieved.

This Part analyzes the approach the United States government is relying on to develop an adequate, effective cybersecurity initiative, i.e., the efforts reviewed in Part III, *supra.* As noted earlier,[438] these efforts commendably focus on remediating factors that contribute to the inefficacy with which existing United States 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.[439]

Part IV.A puts these efforts into context by (i) tracing the United States government's increasing reliance on bureaucracy and (ii) examining the historical and other factors that shaped Weber's views on bureaucracy. Part IV.B then analyzes the efficacy of the efforts outlined in Part III and finds them wanting. Part 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.[440]

The efforts outlined in Part III are all predicated on the bureaucratic model that has come to dominate governance in the U.S. and elsewhere (and also plays a significant role in the

---

438. *See supra* Part II.

439. *See supra* Parts II, III. General Hayden, who was quoted above, seems to agree, at least to some extent. *See supra* note 437. General Hayden also stated:

> We may come to a point where . . . what is permitted there is something that we would never let the private sector do in physical space. . . . [H]ow about a digital Blackwater? . . . [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,* ZDNET (Aug. 1, 2011), http://www.zdnet.com/blog/btl/hayden-digital-blackwater-may-be-necessary-for-private-sector-to-fight-cyber-threats/53639 (quoting General Hayden during a panel discussion in the summer of 2011).

440. MAX WEBER, ESSAYS IN SOCIOLOGY 228 (Hans Gerth & Charles Mills eds. & trans., Galaxy Books 1958) [hereinafter ESSAYS IN SOCIOLOGY].

private sector).[441] We have become accustomed to bureaucracy; it has, in effect, become "business as usual."

In this Part, 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.[442] This can occur in various ways, one of which involves the process of institutionalization.[443]

Institutionalization begins with habitualization: with the development of patterns of human activity that become routinized and are eventually "legitimated."[444] 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.[445] 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."[446] 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.[447]

---

441. *See supra* note 4.

442. *See, e.g.*, PETER BERGER & THOMAS LUCKMANN, THE SOCIAL CONSTRUCTION OF REALITY: A TREATISE IN THE SOCIOLOGY OF KNOWLEDGE 1–3, 89 (1st ed. 1966). The processes by which social phenomena become perceived as objective phenomena that exist separately and independently of human activity is known as reification. *Id.* at 82–83.

443. *See id.* at 45–85.

444. *See id.* at 85–96 (explaining legitimation).

445. *See id.* at 58; *see also id.* at 85–96.

446. *Id.* at 82–83.

447. *See supra* note 442. 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* Wilson, *supra* note 233, at 98 ("Any organization, and *afortiori* any public organization, develops a genuine belief in the rightness of its mission . . . .").

That brings us to our sociology of knowledge exercise, which will proceed in two stages: In the remainder of this subpart, 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 subpart, 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.[448] The New Deal and World War II built upon the earlier increases in the size of United States government bureaucracies, a phenomenon due in large part to the rise of regulatory agencies at both the state and federal levels.[449] As one observer notes, the "growth in the size" of bureaucracy can, to a great extent, be explained by the need for personnel to do "routine, repetitive tasks" the completion of which was essential for various government functions.[450]

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.[451] Max We-

---

448. Wilson, *supra* note 233, at 77. *See also id.* at 87–89 (tracing development of federal and state bureaucracies).

449. *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, 172–73 (2008); Wilson, *supra* note 233, at 78; *see also* Larry G. Gerber, *World War II and the Expansion of Government in America*, 75 NAT'L F. 30 (1995); Cass R. Sunstein, *Constitutionalism after the New Deal*, 101 HARV. L. REV. 421, 421–22 (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." Wilson, *supra* note 233, at 87–91. He also attributes it to the development of federal grants to state and local governments, which resulted in the creation of agencies to monitor the administration and implementation of those grants. *See id.* at 91–93.

450. *See* Wilson, *supra* note 233, 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 FLETCHER F. WORLD AFF. 73, 79 (2004); s*ee 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 . . . .").

451. One author attributes this, at least in part, to the development of

ber would ascribe this persistence of bureaucracy to its efficiency; as I noted earlier,[452] he believed that "[t]he decisive reason for the advance of bureaucratic organization has always been its purely technical superiority over any other form of organization."[453] 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."[454]

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 Part IV.B, I will do something similar, i.e., I will analyze the relative efficacy with which the bureaucracies we examined in Part 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 Part.

Weber was born in 1864; the German Empire became a unified state when he was six years old.[455] In the next forty years, the Empire went through a period of rapid industrialization and population growth.[456] Weber consequently matured in a country that was establishing itself as a modern nation-state and a modern industrial power.[457] He, in fact, became "a cham-

---

"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." Wilson, *supra* note 233, at 93. Wilson also notes that Georg Simmel believed that organizations tend "to acquire the characteristics of those 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.

452. *See supra* note 1 and accompanying text.

453. ESSAYS IN SOCIOLOGY, *supra* note 440, at 214; *see also* WEBER, *supra* note 1, at 337 (stating bureaucracy is the "most rational known means of carrying out imperative control over human beings").

454. *See* WEBER, *supra* note 440, at 214.

455. *See id.* 3–8. *See also* Peter E. Quint, *The Constitutional Law of German Unification*, 50 MD. L. REV. 475, 478 (1991) (describing unification of the German Empire in 1871).

456. *See* VOLKER R. BERGHAHN, IMPERIAL GERMANY, 1871–1914: ECONOMY, SOCIETY, CULTURE AND POLITICS 22–37, 43–54 (1994).

457. *See* Tod Leaven & Christopher Dodge, *The United States Cyber Command: International Restrictions vs. Manifest Destiny*, 12 N.C. J.L. & TECH.

pion of German industrialization."[458]

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 . . . ."[459] 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.[460] 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.[461]

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 the context in which the bureaucracy operates.[462] 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 bi-

---

ONLINE 1, 23 n.132 (2010) ("From 1848 to 1871, the unification of Germany with Prussia brought about a Navy to Rival England, an army to rival any power in Europe, and growing influence to rival the former Hapsburgs.").

458. FRITZ RINGER, MAX WEBER: AN INTELLECTUAL BIOGRAPHY 2 (2004).

459. WEBER, *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." *Id.* at 330–32.

460. *See* RINGER, *supra* note 458, at 64–65, 220–21; *see also* JÜRGEN KOCKA, INDUSTRIAL CULTURE & BOURGEOIS SOCIETY: BUSINESS, LABOR, AND BUREAUCRACY IN MODERN GERMANY 130, 148, 156–57, 198–204 (1999); WEBER, *supra* note 440, at 232 ("Everywhere the modern state is undergoing bureaucratization.").

461. Weber recognized that forms of bureaucratic organization had existed for centuries. *See* ESSAYS IN SOCIOLOGY, *supra* note 440, at 204–24 (describing bureaucracies in ancient Egypt, Rome, and 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 204–28.

462. 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.

furcated approach states use to control threats to internal and external order.[463] 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.[464]

This meant that the state could respectively assign discrete bureaucracies a "specified sphere of competence,"[465] 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.[466] The system was predicated on a multi-faceted division of labor among agencies, with each being the sole arbiter of its sphere of responsibility.[467] 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 Part 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 subpart.

B. THE FALLACY OF INEVITABILITY

The tendency of a principle to expand itself to the limit of its logic . . .[468]

---

463. *See supra* Part II; *see also* WEBER, *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.*

464. *See supra* note 463.

465. WEBER, *supra* note 1, at 330.

466. *See supra* note 459; *see also supra* note 4 (discussing how agencies are concerned with their own turf).

467. *See supra* note 4.

468. BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 51

As we saw in the previous Part, 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.[469] It is the pragmatic product of an ad hoc evolutionary process.[470]

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.[471] Bureaucracy's reliance on hierarchically ordered positions comes from the military, which adopted hierarchical organization several millennia ago.[472] Like the military, modern bureaucracy is based on a tiered organizational structure in which tasks are allocated in order of their decreasing importance to the increasingly less important positions in the bureaucracy.[473] And because authority is allocated in a similar fashion, the functionaries in an organization carry out their duties subject to the supervision and approval of the functionaries above them.[474] As Weber approvingly noted, modern bureau-

---

(1921).

469. *See supra* Part IV.A.

470. *See*, *e.g.*, BERGER & LUCKMANN, *supra* note 442, at 52 ("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, "[a]n 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." *Id.* at 56–57.

471. WEBER, *supra* note 1, at 331; *see supra* note 459.

472. *See, e.g.*, JOHN ARQUILLA & DAVID RONFELDT, SWARMING & THE FUTURE OF CONFLICT 13–14 (2000); s*ee also* ESSAYS IN SOCIOLOGY, *supra* note 440, at 221–24 (discussing the bureaucratization of the army and organized warfare). For non-military uses of bureaucratic organization in the ancient world, see *id.* at 204 (discussing ancient Egypt, Rome, and China). The military developed hierarchical organization to meet its new goal of "achiev[ing] advantages in mass" over an adversary. ARQUILLA & RONFELDT, *supra* note 472, at 13. Hierarchies let commanders create and utilize "well-articulated formations" of troops. *Id.* Hierarchically organized armies therefore replaced the melee, which was the earlier, "chaotic form of war." *Id.* at 10.

473. *See supra* note 459; *see also* ESSAYS IN SOCIOLOGY, *supra* note 440, at 197 ("The principles of office hierarchy and of levels of graded authority mean a firmly ordered system of super- and subordination" in which "lower offices are supervised by higher ones.").

474. *See supra* note 473.

cracy has many of the characteristics of a well-functioning machine.[475]

Machines, as we all know, are well-suited for specific, repetitive tasks but have no ability to adapt to changing circumstances—to innovate.[476] 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.[477]

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.[478] 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.[479] 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.[480]

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 Part III, the federal government's efforts to improve the country's

---

475. *See supra* note 454 and accompanying text.

476. 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.

477. *See, e.g.*, *supra* note 453 and accompanying text.

478. *See supra* note 450 and accompanying text.

479. *See supra* note 4.

480. As to the former, *see supra* note 4. 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 4. 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.

cyber-threat-control structure are all predicated on bureaucratic solutions. So unless we assume the federal government is descending into madness,[481] 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.[482] 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"[483] and, in so doing, implicitly foreclose consideration of alternatives.[484]

I believe the fallacy of inevitability explains the behaviors we reviewed in Part 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 Part III, with the military. As we saw above, the federal government initially intended to im-

---

481. *See Albert Einstein Quotes*, ALBERT EINSTEIN SITE ONLINE, http://www.alberteinsteinsite.com/quotes/einsteinquotes.html (last updated Jan. 8, 2012) ("'Insanity: Doing the same thing over and over again and expecting different results.' -Albert Einstein"). The true origin of this aphorism is unclear and its attribution to Einstein is disputed. *See* Peter Baskerville, *Did Einstein Really Define Insanity as "Doing the Same Thing Over and Over Again and Expecting Different Results"?*, QUORA (Oct. 29, 2010), http://www.quora.com/Did-Einstein-really-define-insanity-as-doing-the-same-thing-over-and-over-again-and-expecting-different-results.

482. *See supra* note 447 and accompanying text; *see also supra* notes 442 and 470 (discussing the definition of reification and how conduct is controlled by setting up predefined patterns of human conduct).

483. BERGER & LUCKMANN, *supra* note 442, at 56.

484. *See id.* at 51 (explaining the institutionalization of behaviors narrows choices and, in so doing, frees us from "the burden of 'all those decisions'").

prove 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.[485] 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. [486]

This initial approach, like all the approaches we examined in Part 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),[487] and thereby avoided the segmented response authority that, among other things, is an integral part of U.S. law enforcement.[488] 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 Parts 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."[489] Cyberspace is a global communication system of tremendous, and continually evolving, complexity and sophistication.[490] It is con-

---

485. *See supra* Part III.A.1.

486. *See supra* Part III.A.1.

487. *See supra* Part II.

488. *See supra* Part III.B; *see also supra* note 3 (discussing how the U.S. law enforcement is segmented into federal, state, and local divisions).

489. See, for example, *Blumenthal v. Drudge*:

> "[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 . . . .

Blumenthal v. Drudge, 992 F. Supp. 44, 48 n.7. (D.D.C. 1998).

490. *See* DEP'T OF DEF., DICTIONARY OF MILITARY AND ASSOCIATED TERMS

sequently impossible to segregate the myriad of activities that create and sustain cyberspace from the real-space actors and assets with which they interact.[491] It would, therefore, have been difficult for the Air Force Cyber Command that was the focus of the initial approach to implement that responsibility.[492] 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.[493] There would therefore have

---

139 (2009), *available at* 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").

491. Each of the five branches of the U.S. military uses cyberspace in its various activities. *See, e.g.*, Joshua E. Kastenberg, *Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the NIPRNET*, 64 A.F. L. REV. 175, 183 (2009) ("During any given twenty-four hour period the Internet is accessed over one billion times from roughly seven million [Department of Defense] owned computers."); *see also Annual Cyber Awareness Training*, MARINES.MIL (Feb. 17, 2011), http://www.marines.mil/news/messages/Pages/MARADMIN118-11.aspx (discussing the annual Cyber Awareness training required for all Department of Defense service members); *Careers*, U.S. AIR FORCE, http://www.airforce.com/careers/#s_computer (last visited Oct. 11, 2012) (listing jobs within the U.S. Air Force, some of which include cyber protection); *Command, Control, Communications, Computers and Information Technology (C4IT) Service Center*, U.S. COAST GUARD, http://www.uscg.mil/c4itsc/ (last modified Sept. 24, 2012) (discussing how C4IT assists the U.S. Coast Guard by providing them the information they need); Gerry J. Gilmore, *Navy Moves to Meet Information Age Challenges*, NAVY.MIL (Oct. 2, 2009, 4:55 PM), http://www.navy.mil/search/display.asp?story_id=48723 (discussing the U.S. Navy's Fleet Cyber Command created to help protect it against cyber-threats); *Network Services: Data*, DEF. INFO. SYS. AGENCY, http://www.disa.mil/services/data.html (last visited Oct. 5, 2012) (describing the Data Services portfolio); Karl Weisel, *Cyber Hawks Help Keep Network Safe*, ARMY.MIL (Aug. 13, 2008), http://www.army.mil/article/11631 (discussing how the U.S. Army monitors cyber-threats). *See generally* Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 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.").

492. *See supra* Part III.A.

493. *See, e.g.*, David M. Hollis, *USCYBERCOM: The Need for a Combatant Command Versus a Subunified Command*, JOINT FORCE Q., 3d Quarter 2010, at 48. Additionally:

> [M]ilitary operations in the cyberspace domain are radically different

been no distinct spatial domain as to which that United States 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 cyber-threats? 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.[494] 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.[495]

> 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.

Id. at 49; s*ee also supra* note 491 (illustrating the use of cyberspace by all military branches).

494. *See supra* Part III.A.

495. *See supra* notes 290–291 and accompanying text (explaining unified commands). 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* Part II.

While it 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.*, Memorandum from Robert Gates, Sec'y of Def., to the Sec'ys of the Military Dep'ts 1 (June 23, 2009), *available at* 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* Hollis, *supra* note 493, at 51 ("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 physical domain, cyber-threat response authority must be unified in one entity. *See id.* at 52. For a description of U.S. Strategic Command, *see supra* notes 237–240 and 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 Department of Defense should adopt the initial, interim step of cre-

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. Strategic Command."[496] And as we also saw above, despite this presumptive integration the branch cyber commands continue to develop and field their respective, idiosyncratic cyberspace capabilities.[497]

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 Command.[498] The capitulation was apparently a victory of turf over logic and pragmatism, a concession to the continuation of business as usual.[499]

---

ating a "subunified command." Hollis, *supra* note 493, at 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." *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.

496. William Jackson, *DOD Creates Cyber Command as U.S. Strategic Command Subunit*, FED. COMPUTER WK. (June 24, 2009), http://fcw.com/Articles/2009/06/24/DOD-launches-cyber-command.aspx?Page=1; *see supra* Part III.A.1.

497. *See supra* note 495; *see also* Part III.A (discussing how each branch of the U.S. military has an interest in protecting the country against cyber-threats and the difficulty in parsing out cyberspace amongst them).

498. *See supra* Part III.A.

499. *See, e.g.*, Peter A. Buxbaum, *US: Cyberwar Turf Battle Continues*, INTELLIBRIEFS (Aug. 30, 2008), http://intellibriefs.blogspot.com/2008/08/us-cyberwar-turf-battle-continues.html (noting that the Air Force's creating its Cyber Command "provok[ed] a turf war with other" branches of the military); Coleman, *supra* note 255 (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 capitulation to turf battles among the various branches of the military. *See Cyber War: Pentagon Takes on Cyber Enemies, Other Agencies*, DEF. INDUSTRY DAILY (Nov. 8, 2011, 23:30 EST), 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 4.

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.[500] 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.[501] 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 U.S. from the cyber-threats for which it 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.[502] 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.[503]

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 bu-

---

I also find inferential support for this assumption in the branches' continuing efforts to develop their own, idiosyncratic cyber-operations plans. *See, e.g.*, Amber Corrin, *Navy's Cyber Unit Scans Horizon for New Challenges*, DEF. SYSTEMS (June 21, 2011), http://defensesystems.com/articles/2011/06/08/cyber-defense-navy-cyber-programs.aspx; *LandWarNet 2011: U.S. Army Detail Cyber Vision 2020*, SHEPHARD NEWS (Aug. 24, 2011, 6:54 PM), http://www.shephardmedia.com/news/digital-battlespace/landwarnet-2011-us-army-detail-cyber-vis.

500. *See supra* Part III.A.

501. *See supra* Part III.A.

502. *See supra* Part III.A; *see also supra* note 499 (discussing how the Air Force's Cyber Command started a turf war).

503. *See supra* Part III.A.1. This article will return to this issue later in this Part.

reaucracy.[504] 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.[505] In other words, Cyber Command's mission is essentially to create its own bureaucratic turf out of turf appropriated from each of the five branches. It is difficult to imagine how it can succeed.[506]

My skepticism is also the product of another of the limitations of bureaucracy, at least when it is 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).[507] As we also saw, this bifurcation has produced a massive series of (i) federal, state and local law enforcement bureaucracies[508] and (ii) military bureaucracies.[509] 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"[510] to each bureaucracy. That means, as we saw earlier, that (i) the military responds only to warfare and (ii) federal, state and local law enforcement responds only to crime or terrorism.[511] 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.[512] 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 cyber-threats 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.[513]

Essentially, the United States military now has a highly-

---

504. *See supra* Part III.A.1.
505. *See supra* Part III.A.1.
506. *See supra* note 4.
507. *See supra* Part II.
508. *See supra* Part III.B.
509. *See supra* Part III.A.
510. WEBER, *supra* note 1, at 330; *see supra* note 459.
511. *See supra* Part II.
512. *See supra* Part III.
513. *See supra* Part II.

articulated, stove-piped[514] system of response authority which is, to say the least, exceedingly problematic when it comes to controlling cyber-threats. Even if we assume, for the purposes of analysis, that Cyber Command 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.[515] 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 the initial attack has ended.[516] It can also, as we saw in Part 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.[517]

Given all that, it is almost certain that criminals, terrorists, and hostile nation-state cyber commands will be able to exploit the huge, elaborately segmented network of bureaucracies described above to their advantage.[518] Bureaucracies tend to move slowly; indeed, I suspect that as a general matter, the speed with which a bureaucracy moves is in inverse proportion

---

514. *See supra* note 4.

515. *See* Robert Vamosi, *Guerrilla Cyber Warfare:Are We Thinking Defensively*, SECURITY WK. (Sept. 1, 2011), http://www.securityweek.com/guerilla-cyber-warfare-are-we-thinking-defensively ("By strongly restricting who has access to the Internet, [a party] can focus its . . . resources on a few [locations] that may be the launch point for [a] cyber attack[] . . . [T]hese are called asymmetric threats . . . ."); Chico Harlan & Ellen Nakashima, *Suspected N. Korean Net Attack Raises Fears*, WASH. POST, Aug. 30, 2011, at A1, A7 ("Cyberwarfare offers high potential for asymmetric threats, providing poor nations with easy opportunities to inflict damage on a richer, more developed rival.").

516. *See* Christopher Williams, *Stuxnet: Cyber Attack on Iran 'Was Carried Out by Western Powers and Israel*, TELEGRAPH (Jan. 21, 2011), http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html.

517. *See, e.g.*, Mark Landler & John Markoff, *After Computer Siege in Estonia, War Fears Turn to Cyberspace*, N.Y. TIMES, May 29, 2007, at A1.

518. See Harlan & Nakashima, *supra* note 515; Williams, *supra* note 516.

to the size and complexity of the bureaucracy.[519] 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 or one or more of its constituent commands 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 Part, we will consider the extent to which the fallacy of inevitability affects United States law enforcement's ability to respond to cyber-attacks.

2. Law Enforcement

As we saw earlier, the bureaucratization of United States law enforcement is to a great extent the product of strictures imposed by our federal system of government:[520] law enforcement agencies are divided into two primary categories—federal and state—and the latter is respectively subdivided into state and local agencies.[521] 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.[522]

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 in the states."[523] That began to change in the "last third of the nineteenth century,"[524] as Congress increasingly used its Commerce Clause power to criminalize conduct that had been prosecutable only at the state level.[525] 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.[526] Notwithstanding

519. In other words, the larger and more complex the bureaucracy, the slower it responds.

520. *See supra* Part III.B; *see also supra* note 3 (discussing subdivision of United States law enforcement).

521. *See supra* Part III.B; *see also supra* note 3.

522. *See supra* note 3.

523. AM. BAR ASS'N TASK FORCE ON THE FEDERALIZATION OF CRIMINAL LAW, THE FEDERALIZATION OF CRIMINAL LAW 6 (1998), *available at* http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=17464.

524. *Id.* at 6.

525. *See id.* at 6.

526. *See, e.g.*, Kathleen F. Brickey, *Criminal Mischief: The Federalization of American Criminal Law*, 46 HASTINGS L.J. 1135, 1142–44 (1995).

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.[527]

As we also saw above, United States law enforcement, unlike the military and private sector entities, has so far not been the target of legislative or other efforts designed to enhance the nation's ability to control cyber-threats.[528] 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,"[529] i.e., crime and terrorism.[530] 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 United States law enforcement agencies operate within a prescribed geographical area:[531] 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.[532] Federal law enforcement agencies' geographical jurisdiction is essentially co-extensive with the United States' territorial jurisdiction.[533] 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 jurisdiction will be limited to the county, municipality or other subdivision of the state that employs them.[534] Each federal, state, or local agency is a bureaucracy because all United States law enforcement agencies were organized, or re-organized, according

527. *See supra* note 3.

528. *See supra* Part III.B.

529. *See* WEBER, *supra* note 1, at 330; *see supra* note 459.

530. *See supra* Part II.

531. *See supra* Part III.B.

532. *See* CHARLES DOYLE, CONG. RESEARCH SERV., 94–166, EXTRATERRITORIAL APPLICATION OF AMERICAN CRIMINAL LAW 1 (2012); *see also id.* at 14–21 (discussing the limited extent that the United States has jurisdiction outside its territory).

533. *See supra* Part III.B. As we saw in Part III.B, federal law enforcement agencies' authorized sphere of investigation is further circumscribed by substantive jurisdictional requirements.

534. *See supra* Part III.B; *see also supra* note 3 (discussing overlap between state and local U.S. law enforcement jurisdictions).

to the principles Weber outlined in his work on bureaucracy.[535]

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.[536] It is also a relatively new phenomenon: the bureaucratization of United States 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.[537] 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.'"[538]

Peel's model became the dominant model of policing in the United States,[539] which brings us to the second factor: Peel's reliance on a quasi-military model as the basis for his police forces.[540] Like members of the military, law enforcement officers wear uniforms[541] and operate within hierarchically-structured organizations that rely on military ranks and a chain of command.[542] 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 physi-

---

535. *See* David J. Bordua & Albert J. Reiss, Jr., *Command, Control, and Charisma: Reflections on Police Bureaucracy*, 72 AM. J. SOC. 68, 70–71 (1966); *see also* Daniel C. Stiles, *Border Crisis: Time for A New Collective Review of Tri-Nation Border Security*, 29 TRANSP. L.J. 299, 307–08 (2002) (discussing how United States law enforcement agencies will re-organize in order to be able to work better with Mexico and Canada); Mark Tushnet & Jennifer Jaff, *Critical Legal Studies and Criminal Procedure*, 35 CATH. U. L. REV. 361, 380–81 (1986) (discussing the implications of having a bureaucratic law enforcement agency).

536. *See supra* Part III.B.

537. *See* David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1202–09 (1999).

538. *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.") (footnotes omitted).

539. *See id.* at 1206–08.

540. *See id*. at 1202.

541. *See id*. at 1207–08.

542. *See id.* at 1202–03; *see also* Bordua & Reiss, Jr., *supra* note 535, at 68–69 (discussing the quasi-military quality of the law enforcement).

cal force in a real-space context.[543] 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 bureaucratic model of organization.[544] This means that bureaucracy is a suitable organizational model when both operate in real-space.[545]

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.[546] The challenges cyberspace creates for law enforcement are the converse of General Alexander's problem,[547] i.e., law enforcement agencies now have to deal with attacks from abroad which can be war, crime, or terrorism.[548]

As I explain elsewhere, the traditional threats—crime, terrorism, and war—can morph in cyberspace,[549] so what appears to be a cybercrime is actually cyberwarfare or cyberterrorism or a hybrid, e.g., cyberwar/crime.[550] As I have also explained, cy-

---

543. *See supra* Part III.B.
544. *See supra* Part IV.A.
545. *See supra* Parts II, IV.A.
546. *See supra* Part III.B.
547. *See supra* Part III.A.
548. *See At Light Speed*, *supra* note 31, at 382–404.
549. *See supra* Part II.
550. *See At Light Speed*, *supra* note 31, at 382–404. The incident I use to illustrate the phenomenon of morphing in cyberspace and the legal conundrums it creates occurred in 2001: Gary Lauck, a United States citizen who lives in Nebraska, was operating websites that distributed pro-Nazi material; distributing such material in Germany is a crime. *See* Susan W. Brenner, *Mixing Metaphors*, CYB3RCRIM3 (Apr. 22, 2009, 6:26 AM), 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. *See id.* 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 United States), 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

berspace eliminates the barriers that historically made warfare the exclusive province of nation-states;[551] it is therefore not only possible but likely that non-nation-state actors will launch cyber-attacks that are intended to undermine the sovereign viability of a nation-state, i.e., attacks that are indistinguishable from warfare.[552]

United States law enforcement agencies have traditionally been responsible for controlling crime and terrorism.[553] They are neither authorized to, nor capable of, responding to acts of war, including cyberwar.[554] And aside from anything else, it would not be prudent for the U.S. to alter this state of affairs and authorize its law enforcement officers to respond to cyber-

---

is supported, however, by the fact that Germany's hypothesized cyber-attack 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 had the hypothesized attack happened it 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 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 United States could have charged him with cybercrime and asked the German authorities to extradite him for prosecution in the United States. *See id.*

551. *See supra* Part II.

552. *See, e.g.*, Landler & Markoff, *supra* note 517; *see also At Light Speed*, *supra* note 31, at 422–23; *US Standards Body Issues Warning to Energy Suppliers over Cyber Attacks*, INFOSECURITY (Aug. 8, 2011), http://www.infosecurity-magazine.com/view/19930/us-standards-body-issues-warning-to-energy-suppliers-over-cyber-attacks (discussing how many utility companies were vulnerable to outside cyber-attack).

553. *See supra* Part 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.") (footnotes 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.

554. *See supra* Part II.

attack 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-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.[555]

The United States and other nation-states therefore confront both a problem and a dilemma: the problem, as we saw in Part 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 cyber-attack (i) is from abroad or is a domestically-based attack that has been routed through foreign servers to disguise its true nature and (ii) is crime, terrorism, or warfare.[556] This impedes the military's ability to respond with the speed, discrimination, and efficacy needed to deter attacks from hostile nation-states.[557] 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

---

555. 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, 7:17 AM), http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare/8686.

556. *See Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law*, U.S. DEP'T OF JUST. (May 20, 2011), http://www.justice.gov/criminal/pr/testimony/2011/crm-testimony-110510.html; *see supra* Part II.

557. *See supra* Parts III.A.2 and IV.A.2.

if a cyber-attack (i) is domestic or originated from abroad and (ii) is crime, terrorism, or warfare.[558] Their respective problems interact to create uncertainty as to whether a particular cyber-attack falls within law enforcement's or the military's "sphere of competence."[559]

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 eroded the country's ability to maintain internal or external order.[560] If both respond, this could result in an unintended escalation of the situation, e.g., if a cybercriminal attacks a United States bank and becomes the target of retaliative action by United States law enforcement and the United States military, the latter's involvement could escalate the incident to cyberwarfare.[561]

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 United States military "from performing a domestic civilian law enforcement function."[562] The Posse Comitatus Act is one of the bulwarks of the bifurcated approach to threat-control we examined in Part II, but it is merely the product of legislative action; we could repeal the Act, thereby

---

558. *See supra* Part II. *See Statement of Deputy Assistant Attorney General Jason Weinstein Before the Senate Judiciary Subcommittee on Privacy, Technology and the Law*, *supra* note 556 ("Investigating . . . multi-actor, multinational crimes is extremely resource intensive.").

559. *See* WEBER, *supra* note 1, at 330; *see supra* note 459.

560. 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 Distributed Security*, *supra* note 29, at 691 (noting that utility of sanctions in deterring criminal conduct is a function of the perceived risk of being caught); *see also Criminal Law for Cyberspace*, *supra* note 7, at 60 (discussing "control by deterrence"); Harold G. Grasmick & Robert J. Bursik, Jr., *Conscience, Significant Others, and Rational Choice: Extending the Deterrence Model*, 24 LAW & SOC'Y REV. 837, 841 (1990) (discussing three possible costs for committing a crime: deprivation, shame, and embarrassment); Margaret Raymond, *Penumbral Crimes*, 39 AM. CRIM. L. REV. 1395, 1404 (2002) (discussing how the "threat of enforcement acts as a deterrent").

561. *See supra* note 550.

562. Mark David "Max" Maxwell, *The Enduring Vitality of the Posse Comitatus Act of 1878*, 37 PROSECUTOR 34, 34 (May/June 2003); 18 U.S.C. § 1385 (2006).

eliminating the statutory provision that bars the integration of civilian and military personnel. Since no correlate provision bars United States law enforcement from assisting the military,[563] 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,"[564] a sentiment to which the nation's founders clearly subscribed.[565] 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,[566] 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 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 cyber-threat: I fear the impact the fallacy of inevitability would have on such a step. Absent a dramatic and 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.[567] That would only ex-

---

563. *See At Light Speed, supra* note 31, at 444–55.

564. Scott R. Tkacz, *In Katrina's Wake: Rethinking the Military's Role in Domestic Emergencies*, 15 WM. & MARY BILL RTS. J. 301, 307 (2006).

565. *See id*. at 327; *see also* William C. Banks, *The Normalization of Homeland Security After September 11: The Role of the Military in Counterterrorism Preparedness and Response*, 64 LA. L. REV. 735, 741 (2004) (detailing the Posse Comitatus Act is "a symbol of our nation's subordination of military to civilian control, and to the distaste of military involvement in domestic law enforcement"); Nathan Canestaro, *Homeland Defense: Another Nail in the Coffin for Posse Comitatus*, 12 WASH. U. J.L. & POL'Y 99, 99 (2003) (noting this separation is "derived from a long tradition of antimilitarism in English common law, [it] represents the 'traditional and strong resistance of Americans to any military intrusion into civilian affairs.'") (footnote omitted).

566. *See, e.g.*, CYBER-THREATS, *supra* note 7, at 294.

567. We might, as I note elsewhere, refer to it as the Cyber Security Agency. *See id*. at 293–95.

acerbate 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.[568] 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.[569]

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

3. Civilians

As we saw in Part 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.[570] 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.[571] 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 or cyberterrorism but are in reality attacks designed to advance a sovereign's covert agenda, i.e., cyberwarfare.[572] The result, to paraphrase William Yeats, is that things threaten to fall apart and anarchy seems a viable prospect.[573]

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, are now on the front line of cyber conflict.[574] Civilians have for

---

568. *See supra* Part III.

569. *See supra* Part IV.

570. *See supra* Part II.

571. *See supra* Part II.C.2.

572. *See* Danchev, *supra* note 555 and accompanying text.

573. *See* WILLIAM BUTLER YEATS, *The Second Coming*, *in* THE COLLECTED POEMS OF W.B. YEATS: A NEW EDITION 187 (Richard J. Finneran ed., 1989).

574. *See, e.g.*, J. Ricou Heaton, *Civilians at War: Reexamining the Status of*

years been the targets of cybercrime;[575] civilian entities may have been, and most certainly will be, the targets of cyberterrorism and cyberwarfare.[576] This means that at least some civilians will have to participate in cyber-conflict,[577] a reality the legislative proposals we examined in Part III.C.1 all acknowledge.

The 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 Part is to explain how, and why, the approach the proposals we examined in Part 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 Part 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.[578] In this Part, 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.[579]

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

---

Civilians Accompanying the Armed Forces, 57 A.F.L. REV. 155, 157–63 (2005).

575. *See* BRENNER, *supra* note 361, at 9–37.

576. *See, e.g.*, RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT, at xi (2010) ("The most likely targets [of cyberwarfare] are civilian in nature . . . ."); *see also id.* at xiii ("[I]t 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 At Light Speed*, *supra* note 31, at 426–27, 454–55 (noting that civilian computers are the targets of cyberwarfare).

577. I use the generic term cyber-conflict because, as we saw above, it will be difficult to parse attacks into cybercrime, cyberterrorism and cyberwarfare. *See supra* Part II.C.

578. 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, *supra* note 387, at 1–7. It also includes provisions governing data breach notification. *See id.* at 8–18.

579. *See supra* Part IV.B.

ability to avoid or withstand cyber-attacks and (ii) plans for responding to cyber-attacks.[580] The entities will be required to comply with these requirements as long as their company is deemed to be part of the nation's critical infrastructure.[581] And as we saw in Part 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.[582] As I explained earlier, this approach is, as a general matter, flawed when it is utilized in an effort to address cyber-threat.[583] 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.[584] 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.[585] The same is true of businesses, educational institutions, and government agencies charged with carrying out other specific tasks (e.g., FEMA and similar enti-

---

580. *See supra* notes 375–377 and accompanying text. As I noted earlier, the precise nature of the plans for responding to cyber-attacks is not specified. *See supra* notes 414–415 and accompanying text.

581. *See, e.g.*, Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 254(c)(3) (2011).

582. 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 459.

583. *See supra* Part IV.A.

584. *See, e.g.*, WILSON, *supra* note 4, at 25 (noting that bureaucracies are charged with carrying out certain "critical tasks").

585. *See supra* Part IV.A.

ties).[586]

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.[587] 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 functions.[588] When Weber approvingly described bureaucracies as machines, he was referring to implementary bureaucracy.[589]

---

586. *See* Stephen M. Bainbridge, *Participatory Management Within a Theory of the Firm*, 21 J. CORP. L. 657, 674 (1996) ("Taylorism and the comparable forms of scientific management pioneered by Henry Ford and others designed firms as highly centralized, hierarchical bureaucracies."); *see also* U.S. DEP'T OF HOMELAND SEC., FED. EMERGENCY MGMT. AGENCY, NATIONAL RESPONSE FRAMEWORK 47–69 (2008), *available at* http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (detailing the hierarchical organization of staff roles in the National Response Framework).

587. *See supra* Part IV.B.

588. *See supra* text accompanying notes 465–466. 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, *Medellin, Delegation and Conflicts (of Law)*, 17 GEO. MASON L. REV. 191, 206 (2009). As Rutledge 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. *Id.* at 206 n.74. 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*, HARV. NAT'L SECURITY J. (Nov. 15, 2010, 12:11 AM), http://harvardnsj.com/2010/11/dod-dhs-memorandum-of-understanding-aims-to-improve-cybersecurity-collaboration. *See generally* WILSON, *supra* note 4 (discussing what government agencies do and how they do it).

589. *See supra* note 475 and 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* to MAX WEBER, THE THEORY OF SOCIAL AND ECONOMIC ORGANIZATION, 12–13 (Talcott Parsons ed., A. M. Henderson & Talcott Parsons trans., First Free Press Paperback Edition 1964). Parsons explains Weber's ideal type as follows:

> 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

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.[590] The Federal Aviation Administration, for example, "promote[s] civil aviation, promulgate[s] safety regulations, and establish[es] and enforce[s] air traffic and navigational rules" in the U.S.[591] 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."[592]

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.[593] The regulatory bureaucracies' charge

---

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 471–475 and accompanying text. I also base this assertion on 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.*, Wilson, *supra* note 233, at 94–98 (discussing the emergence of regulatory bureaucracy in the United States).

590. *See, e.g.*, *General Information*, ONT. PUB. APPOINTMENTS SECRETARIAT, http://www.pas.gov.on.ca/scripts/en/generalinfo.asp#1 (last modified Aug. 23, 2012) ("Regulatory agencies make independent decisions (including inspections, investigations, prosecutions, certifications, licensing, rate-setting, etc.) which limit or promote the conduct, practice, obligations, rights, responsibilities, etc. of an individual, business or corporate body."). The description of regulatory agencies 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 587–589 and accompanying text.

591. Matthew J. Kelly, Comment, *Federal Preemption by the Airline Deregulation Act of 1978: How Do State Tort Claims Fare?*, 49 CATH. U. L. REV. 873, 876 (2000) (citing Pub. L. No. 85-726, § 103, 72 Stat. 731, 740 (1958)); *see also id.* at 876–77 (describing the creation of the Federal Aviation Administration); *History*, FED. AVIATION ADMIN., http://www.faa.gov/about/history/brief_history/ (last updated Feb. 1, 2010) (describing the history of the Federal Aviation Administration).

592. *What We Do*, FED. COMM. COMMISSION, http://www.fcc.gov/what-we-do (last visited Oct. 5, 2012).

593. *See, e.g.*, *FCC Rulemaking*, FED. COMM. COMMISSION, http://www.fcc.gov/rulemaking (last visited Oct. 5, 2012). *See also supra* note

is to ensure that the implementary agencies subject to their jurisdiction carry out the tasks assigned to them in a safe, effective manner.[594] 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.[595]

The Department of Homeland Security-based bureaucracy that would be created by the proposals we examined in Part III.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,[596] it would not be directly charged with protecting the United States and its citizens from threats originating here or abroad; instead, the proposed Department of Homeland Security-based 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 essential for the country's survival and prosperity.[597]

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

---

590 and accompanying text (characterizing regulatory bureaucracies).

594. For example:

> [Hawkins and Thomas draw the] rough but necessary distinction between [regulatory] "policy formation"—a "process whereby the agency interprets and translates legislative goals into rules, standards, and plans of action—and "implementation"—"enforcement of 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."

Daniel Richman, *Prosecutors and Their Agents, Agents and Their Prosecutors*, 103 COLUM. L. REV. 749, 757 n.30 (2003) (quoting Keith Hawkins & John M. Thomas, *The Enforcement Process in Regulatory Bureaucracies*, *in* ENFORCING REGULATION 3, 10 (Keith Hawkins & John M. Thomas eds., 1984)).

595. *See supra* notes 459–461 and accompanying text.

596. *See supra* Part II.A and Part III.A–B.

597. *See supra* notes 385–388 and accompanying text. 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* Part III.C.1.

of responsibility for protecting the country from cyber-threats.[598] As we saw in Part 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.[599]

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.[600] 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 cyber-threat control) (ii) but would be responsible for imposing a new non-civilian function, or set of functions, on these entities.[601] 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.[602] The authors of the Senate proposals clearly recognized that entities are likely to resist being conscripted into this effort, because they included a 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 Depart-

---

598. *See supra* note 580 and accompanying text.

599. *See supra* note 385 and accompanying text; *see also supra* Part III.C (outlining the requirements of proposed cybersecurity legislation).

600. *See, e.g.*, Casey B. Mulligan & Andrei Shleifer, *Conscription as Regulation*, 7 AM. L. & ECON. REV. 85, 88 (2005) (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* Brenner & Clarke, *supra* note 40, at 1049–57; Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Casualties*, 13 SMU SCI. & TECH. L. REV. 249, 268–82 (2010) [hereinafter *Civilians in Cyberwarfare*].

601. *See supra* text accompanying note 598. For some thoughts as to how this might be structured, *see* Brenner & Clarke, *supra* note 40, at 1056–62.

602. Unlike traditional military conscripts, their status would not shift entirely from civilian to member of the United States military. *See* Brenner & Clarke, *supra* note 40, at 1056–62. 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.* at 1064–66. *See also Civilians in Cyberwarfare*, *supra* note 600, at 253–54 (suggesting a framework for separating certain aspects of civilian life from obligations of conscription).

ment of Homeland Security bureaucracy.[603]

I see at least three significant flaws in the approach the Senators and the White House are taking to the task of enhancing the U.S.'s ability to control cyber-threats.[604] 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 Part 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 cyber-threats. It implicitly, and incorrectly, assumes that the strategy nation-states rely on to control real-space threats can be effective in controlling cyber-threats.[605] As we saw in Part II, while this strategy has been effective in controlling territorially-based threats, it is not an effective approach to controlling cyber-threats.

That brings us to the third flaw: because it is predicated on 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.[606] 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

---

603. *See, e.g.*, Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 254(c)(2) (2011) (stating that an owner or operator of a system or asset identified as covered critical infrastructure may file an appeal "seeking judicial review" of the entity's "final agency action" in the U.S. District Court for the District of Columbia).

604. As I noted above, other members of Congress have submitted their own cybersecurity legislative proposals. *See supra* notes 389–392 and accompanying text. Since those proposals are similar in at least certain respects to the White House and Senate proposals, we will not examine them separately.

605. *See supra* Part II.

606. *See supra* note 459.

are subject to the organization's supervision.[607] As we saw in Part 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 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*.[608] 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 would impose on these entities would alter their routine functioning and mission in various ways and would, as a result, almost certainly generate resistance.[609] That means these measures, like any prescriptive rules,[610] 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 the implementation of these measures, effective enforcement would be an incredibly complex, challenging, and expensive undertaking.[611]

It would almost certainly be ineffective. In Part 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

---

607. *See supra* note 459. 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 *Distributed Security*, *supra* note 29, at 659, 690–91.

608. Weber emphasized the role discipline played in the effectiveness of military bureaucracy. *See* ESSAYS IN SOCIOLOGY, *supra* note 440, at 261; *see also* TALCOTT PARSONS, THE STRUCTURE OF SOCIAL ACTION 507 (2d ed. 1968) ("Above all bureaucracy involves discipline.").

609. *See, e.g.*, Brenner & Clarke, *supra* note 40, at 1058–60 (discussing the effect on corporations of conscription of the company and its employees).

610. *See supra* note 607.

611. For the difficulties involved in enforcing a much simpler set of cybersecurity rules, see *Criminal Law for Cyberspace*, *supra* note 7, at 90–95.

efficacy of this system by blurring the distinction between "inside" (crime/terrorism) and "outside" (warfare) threats. 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, it is not an effective means of organizing technologically-mediated activities.[612]

Networks are lateral, fluid systems. Social networks—the informal associations of individuals that arise in cyberspace[613]—usually have no fixed structure, constituency or endurance.[614] They are often opportunistic, i.e., they emerge for a more or less specific reason and dissipate when that imperative declines or disappears.[615] Social networks of whatever size and constituency have proven quite effective in evading law enforcement and military bureaucracies.[616] Their success in this regard is, as we saw in Part 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 Part 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 Parts II and III, sovereigns have long re-

---

612. *Distributed Security*, *supra* note 29, at 668 (footnotes omitted). For the link between hierarchical organization and real-world activity, see *Criminal Law For Cyberspace*, *supra* note 7, at 78–79.

613. *See About Us*, ANONYMOUS ANALYTICS, http://anonanalytics.com (last visited Oct. 6, 2012) ("Anonymous is a decentralized network of individuals . . . .").

614. *See, e.g.*, *id.*; *see also* Cassell Bryan-Low & Siobhan Gorman, *Inside the Anonymous Army of 'Hacktivist' Attackers*, WALL ST. J., June 23, 2011, at A1, A14 ("While there may be a hundred or so followers of a network on a regular basis, numbers swell into the thousands during popular campaigns.").

615. *See, e.g.*, Bryan-Low & Gorman, *supra* note 614, at A14.

616. *See, e.g.*, *id.*

lied 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 Part 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 Part 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 is a criminal, terrorist, state warrior, or non-state warrior, (iii) where he is or was when the attack was launched, and (iv) whether launching a responsive cyber-attack would violate United States law, international law, 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.[617] 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 day,[618] 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.[619] 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 Part II, that will not be true; online attacks vary in (apparent) place of origin, nature, duration, objective, and a number of other factors.[620] They can also evolve very quickly, which would make the proposed bureaucracy's task even more difficult.[621]

---

617. *See supra* Part II.

618. *See, e.g.*, *CBS Evening News with Scott Pelley: First Look Inside the Military's Cyber War Room* (CBS television broadcast July 14, 2011), *available at* http://www.cbsnews.com/stories/2011/07/14/eveningnews/main20079585.shtml.

619. *See, e.g.*, Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 101(a) (2011).

620. *See supra* Part II.

621. *See At Light Speed*, *supra* note 31, at 379 n.1 (quoting THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE at xii, 2 (2003)), *available at* http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

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.[622] 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 cyber-attacks.[623] Absent such coordination, they are, at best, likely to duplicate their respective efforts and, at worst, to interfere with those efforts.[624]

I could note other problems with the proposals we examined in Part 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 mechanism in a non-spatial context in which such exercises are meaningless. In the next Part, I outline an alternative approach, one that has its own challenges.

V. . . . AND BEYOND?

That it have been ufed fo long, that the memory of man runneth not to the contrary.[625]

My primary purpose in writing this article is to explain why our persistent reliance on Weberian bureaucracies as the

---

("Cyber-attacks cross borders at light speed . . . .").

622. As we saw in Part III, neither of these is a unitary entity: Cyber Command encompasses the five subordinate cyber commands and United States law enforcement encompasses agencies at the federal, state and local levels. *See supra* Part III and note 3. 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 Part III.C.

623. *See* Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. § 242 (2011); White House, Cybersecurity Proposal, *supra* note 387.

624. 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.

625. I WILLIAM BLACKSTONE, COMMENTARIES *76 (noting that the authority of the common law derived from its long usage).

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.[626]

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.[627] 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*;[628] I cannot understand why knowledgeable people in government and in the private sector do not

---

626. *See, e.g.*, *Criminal Law for Cyberspace*, *supra* note 7, at 105–06.

627. *See supra* Part IV.A.

628. HANS CHRISTIAN ANDERSEN, *The Emperor's New Clothes*, *in* ANDERSON'S FAIRY TALES 79 (Jean Hersholt trans., 1942), *available at* http://www.andersen.sdu.dk/vaerk/hersholt/TheEmperorsNewClothes_e.html.

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-down, hierarchically organized system.[629] 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.[630] 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.[631] Essentially, all of the adult, able-bodied males in a community were in charge of fending off external threats and controlling internal threats.[632] The colonists brought this system with them to the United States, where it survived into the nineteenth century, when it was re-

---

629. *See* note 626 and accompanying text.

630. *See Criminal Law for Cyberspace*, *supra* note 7, at 61 ("The disintegration of the Roman Empire plunged Europe into chaos; social systems that had relied on Roman institutions were forced to resort to older measures to maintain order.").

631. *See id.* at 61–62 (describing the Saxonty thingman and shire reeve systems as the equivalent to modern law enforcement).

632. For a more detailed account of the origins and operation of this system, see, for example, CYBER-THREATS, *supra* note 7, at 165–75. *See also Criminal Law for Cyberspace*, *supra* note 7 at 61–63; Brenner & Clarke, *supra* note 40, at 1074–75; *see*, *supra* note 537, at 1165, 1195 (describing the community-based origins of Anglo-American law enforcement, requiring "every adult male" to participate). If a qualified male member of the community failed to participate in this system, he was subject to punishment. *See* CYRIL D. ROBINSON ET AL., POLICE IN CONTRADICTION: THE EVOLUTION OF THE POLICE FUNCTION IN SOCIETY 92 (1994) ("Failure to participate or the breach of rules could result in fine or outlawry.").

placed by the formal institutions we rely on today.[633]

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.[634] 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).[635] 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 Part 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 there are several reasons why we should not.[636]

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 cyber-threats, like crimes and acts or terrorism and acts of war, have an identifiable dynamic and

---

633. *See, e.g.*, CYBER-THREATS, *supra* note 7, at 165–75; *Criminal Law for Cyberspace*, *supra* note 7, at 61–63; *see also supra* Part II (describing current formal enforcement institutions).

634. *See supra* note 630.

635. *See, e.g.*, *At Light Speed*, *supra* note 31, at 445–46.

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

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.[637] 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;[638] 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 British took to controlling the real-space threats they confronted.

We explored the flaw in the second assumption in Part 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.[639]

---

637. *See supra* Part II.

638. *See supra* notes 575 and 576 and accompanying text.

639. 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 632. 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.*, *Criminal Law for Cyberspace*, *supra* note 7, at 105–07; *see also* Susan W. Brenner, *Toward a Criminal Law for Cyberspace: Product Liability and Other Issues*, 5 U. PITT. J. TECH. L. & POL'Y, Fall 2004, at i, 50–63 (describing theories of civilian responsibility in preventing cybercrime).

That brings us back to the issue I noted earlier:[640] 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.[641]

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.[642] 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.[643]

---

640. *See supra* notes 432 and 433 and accompanying text.

641. One article describes the prevailing corporate attitude as follows:

> You need to consider: What are the subconscious assumptions that companies bring to the issue of foreign cyber-attacks on their networks? … 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 . . . .

Gross, *supra* note 395, at 234 (quoting a senior Senate staffer who works on cyberissues). I suspect we will see the disinclination eroded gradually, as news outlets and other media publicize leaked information about cyber-attacks and, in so doing, begin to cultivate attitudes similar to those that have driven many citizens to invest in alarm systems and burglar bars.

642. 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 415 and 420 (noting current focus on defensive measures and potential benefits of offensive measures).

643. *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 following premise:

> 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 na-

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.[644] 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.

> tional 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 ASSOCIATED UNIVS., INC., PART I OF THE REPORT OF THE PROJECT EAST RIVER 9 (1952)).

644. 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.