2014

# Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation

David G. Delaney
*Indiana University Maurer School of Law*, dgdelane@indiana.edu

# CYBERSECURITY AND THE ADMINISTRATIVE NATIONAL SECURITY STATE: FRAMING THE ISSUES FOR FEDERAL LEGISLATION

*David G. Delaney*[1]

Abstract

In the digital age, every part of federal government has critical cybersecurity interests. Many of those issues are brought into sharp focus by Edward Snowden's disclosure of sensitive government cyber intelligence programs conducted by the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligence Agency. Courts are reviewing various constitutional and statutory challenges to those programs, two government review groups have reported on related legal and policy issues, and Congress is considering cyber intelligence reform proposals. All of this action comes on the heels of significant efforts by successive administrations to restructure government and pass comprehensive cybersecurity legislation to improve the nation's posture to strategically address cyber issues. This Article proposes that new framework legislation is needed to comprehensively address issues relating to Snowden's disclosures and broader cybersecurity interests.

## I. Introduction

### A. Cybersecurity

Cybersecurity can be understood as efforts to secure digital information, the equipment that processes that information, and the means of transmitting that information among devices. At its core, cybersecurity involves information security or assurance—preserving the confidentiality, availability, and integrity of information.[2] This field is sometimes expanded to include authenticity, accountability, non-repudiation, reliability and resilience.[3]

But the term is also shaped and informed by perspectives on cyberspace—the zones beyond an entity's own networks that affect security of its information.

---

1. Visiting Assistant Professor of Law, Indiana University Maurer School of Law, and former Deputy Associate General Counsel, U.S. Department of Homeland Security. Toby Sedgwick and Antonina Semivolos deserve special thanks for their invaluable research assistance.

2. Lukas Feiler, *Information Security Law in the EU and the U.S.: A Risk-Based Assessment of Regulatory Policies*, 8 (2011), *available at* http://www.law.stanford.edu/publications/information-security-law-in-the-eu-and-the-us-%E2%80%94-a-risk-based-assessment-of-regulatory-policies.

3. *Id.* at 15; Federal Information Security Management Act of 2002, 42 U.S.C. § 3542(b)(1) [hereinafter FISMA].

Government entities delivering public services[4] and private entities conducting business via the Internet, mobile devices, and electronic connections take strategic approaches to managing cyber risk. These strategies increasingly include proactive, operational steps to secure or defend computer networks. The Department of Homeland Security (DHS) established a "continuous diagnostics and mitigation" program in conjunction with the General Services Administration (GSA) to enable federal, state, local, and regional governments "to provide a consistent, government-wide set of continuous diagnostic solutions to enhance defenders' abilities to identify and mitigate emerging cyber threats through risk-based decision making."[5] The U.S. Cyber Command defends networks in military, not merely administrative, terms.[6] And private companies increasingly pursue "active defense" strategies to identify and prevent specific cyber threat actors.[7] These approaches reflect a common interest in pursuing all available legal and technological means to identify, prevent, and disrupt cybersecurity concerns as early and efficiently as possible, preferably well before the threats reach an entity's networks.

These concepts of cybersecurity and cyberspace are joined as much in broad national strategies as in practice for public and private entities. The Department of Defense (DOD) identified cyberspace as a new domain of warfare in 2011.[8] DHS asserts that "[o]ur daily life, economic vitality, and national security depend on a

4. *See, e.g.*, FISMA, 44 U.S.C. § 3541 *et seq.*; MEMORANDUM M-14-03 FROM THE DIRECTOR OF THE OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SP 800-37 REVISION 1, "GUIDE FOR APPLYING THE RISK MANAGEMENT FRAMEWORK TO FEDERAL INFORMATION SYSTEMS A SECURITY LIFE CYCLE APPROACH" (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SP 800-39, "MANAGING INFORMATION SECURITY RISK: ORGANIZATION, MISSION, AND INFORMATION SYSTEM VIEW" (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

5. U.S. COMPUTER EMERGENCY READINESS TEAM, CONTINUOUS DIAGNOSTICS AND MITIGATION, http://www.us-cert.gov/cdm (last visited Apr. 21, 2014). *See also*, U.S. DEPARTMENT OF HOMELAND SECURITY, CONTINUOUS DIAGNOSTICS AND MITIGATION, http://www.dhs.gov/cdm (last visited Apr. 21, 2014); U.S. GENERAL SERVICES ADMINISTRATION, CONTINUOUS DIAGNOSTICS AND MITIGATION, http://www.gsa.gov/portal/content/176671?utm_source=FAS&utm_medium=print-radio&utm_term=cdm&utm_campaign=shortcuts (last visited Apr. 21, 2014).

6. *See* DEPARTMENT OF DEFENSE, STRATEGY FOR OPERATING IN CYBERSPACE, 5-7 (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf [hereinafter DOD CYBER STRATEGY]; U.S. CYBER COMMAND, FACTSHEET, http://www.stratcom.mil/factsheets/2/Cyber_Command ("The Command has three main focus areas: Defending the DoDIN [Department of Defense information networks], providing support to combatant commanders for execution of their missions around the world, and strengthening our nation's ability to withstand and respond to cyber attack.") (last visited Apr. 21, 2014).

7. *See, e.g.*, Tom Bowers, *Time For An 'Active Defense' Against Security Attacks*, INFORMATION WEEK DARK READING, Dec. 12, 2013, http://www.darkreading.com/security-monitoring/time-for-an-active-defense-against-security-attacks/d/d-id/1113011; Press Release, *CrowdStrike Launches Big Data Active Defense Platform*, June 18, 2013, http://www.prnewswire.com/news-releases/crowdstrike-launches-big-data-active-defense-platform-211954701.html; CrowdStrike Blog Post, *Active Defense: Time for a New Security Strategy*, Feb. 25, 2013, http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/.

8. *See* DOD CYBER STRATEGY, *supra* note 6, at 5. *See also* U.S. DEP'T. OF DEF., THE CYBER DOMAIN: SECURITY AND OPERATIONS, http://www.defense.gov/home/features/2013/0713_cyberdomain/ (last visited Apr. 21, 2014) (providing links to information about the cyber forces of the military services, DOD cyber research, cyber education for the service academies, cyber speeches of senior DOD and intelligence officials, and other DOD and federal cyber entities).

stable, safe, and resilient cyberspace."[9] Law enforcement efforts to investigate crime and reduce threats in cyberspace are categorized as cybersecurity risk management objectives, not merely cybercrime, counterterrorism, or counterintelligence functions.[10] And since 9/11 each President has issued national cyber policies and directives that identify international, economic, and regulatory objectives for cyberspace and cybersecurity.[11] In these documents the private sector is identified as a primary developer of new technology, partner in developing the U.S. and global economies, and source of expertise on emerging norms for the development and regulation of cyberspace. Cybersecurity thus comprises many interdependent, public-private, domestic-foreign, and military-civilian national interests.

## B. The Snowden Disclosures

Cyber intelligence programs of the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Central Intelligence Agency (CIA) are at the center of public disclosures by Edward Snowden, a former NSA contractor. In this Article, the term "cyber intelligence programs" refers to the programs and investigations of these agencies and other elements of the U.S. intelligence community that are conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA),[12] Executive Order 12,333,[13] or other sources of law regulating intelligence actions.[14] This term includes widely reported programs like the NSA's bulk telephony metadata or "business records" program conducted pursuant to

---

9. U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY OVERVIEW, http://www.dhs.gov/cybersecurity-overview (last visited Apr. 21, 2014) (providing information about "the cyber ecosystem," responding to cyber vulnerabilities, cybersecurity, cyber crime, privacy, and cybersecurity partnerships).

10. *See* WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 9 (2011) *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 21: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

11. *See, e.g.,* WHITE HOUSE, NATIONAL STRATEGY TO SECURE CYBERSPACE (2003); WHITE HOUSE, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative ("The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.") Exec. Order No. 13,636 § 1, 78 Fed. Reg. 11737 (Feb. 19, 2013); WHITE HOUSE, NATIONAL SECURITY STRATEGY (2012), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

12. Pub. L. No. 95–511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. § 1801 *et seq.*) [hereinafter FISA].

13. Exec. Order No. 12,333, 46 Fed. Reg. 59941 .

14. *See, e.g.,* National Security Act of 1947, Pub. L. No. 80-253, 61 Stat. 495 [hereinafter National Security Act]; 12 U.S.C. § 3414 (2006); 18 U.S.C. § 2709 (2006); 50 U.S.C § 3162 (2006) (authorizing administrative subpoenas or "National Security Letters" for intelligence purposes).

section 215 of the USA PATRIOT Act,[15] the NSA's PRISM program conducted pursuant to FISA section 702,[16] the CIA's financial information program pursuant to section 215,[17] and the FBI's roles in these programs.[18] It also includes programs that remain outside the public view or, like the NSA's now-defunct bulk pen register/trap and trace collection program authorized by FISA,[19] on the fringes of the public dialog.

Snowden's disclosures have not touched upon the additional, non-intelligence cyber activities that these and other government agencies conduct under a variety of other legal authorities. For example, the FBI investigates cybercrime and conducts significant cybersecurity outreach to the private sector in all fifty-six U.S. field offices as a function of its combined law enforcement, infrastructure protection, and intelligence functions.[20] Through a combination of federal law and presidential directives, the NSA provides information security expertise to the defense community[21] and administers the government-wide information security program for "national security systems,"[22] which handle information classified according to

---

15. *See, e.g.*, WHITE HOUSE, LIBERTY AND SECURITY IN A CHANGING WORLD; REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, 79-89, 94-98, (2013), *available at* www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter LIBERTY AND SECURITY IN A CHANGING WORLD] (discussing the history of section 215 and its use to obtain business records of individuals); Order, "*In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [TEXT REDACTED]," Docket No. BR (FISA Ct. April 25, 2013) [hereinafter FISC Order of April 2013], *available at* http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

16. 50 U.S.C. § 1881a (2008).

17. Charlie Savage & Mark Mazzetti, *C.I.A. Collects Global Data on Transfers of Money*, N.Y. TIMES, Nov. 14, 2013, http://www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html; Siobhan Gorman, Devlin Barrett & Jennifer Valentino-Devries, *C.I.A.'s Financial Spying Bags Data on Americans: Information on International Money Transfers Includes Financial and Personal Data of Americans*, WALL ST. J., Jan. 25, 2014,
http://online.wsj.com/news/articles/SB10001424052702303559504579198370113163530.

18. FISC Order of April 2013, *supra* note 15; Shane Harris, *Meet the Spies Doing the NSA's Dirty Work*, FOREIGN POLICY, Nov. 21, 2013,
http://www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work.

19. 50 U.S.C. § 1841-1846 (1978); *See also*, LETTER FROM RONALD WEICH, ASSISTANT ATT'Y GEN. TO THE HONORABLE SILVESTRE REYES, CHAIRMAN, PERMANENT SELECT COMMITTEE ON INTELLIGENCE, U.S. HOUSE OF REPRESENTATIVES (2009), *available at*
http://www.dni.gov/files/documents/2009_CoverLetter_Report_Collection.pdf ("We agree that it is important that all Members of Congress have access to information about [the Section 215 "business records" program], as well as a similar bulk collection program conducted under the pen register/trap and trace authority of FISA, when considering reauthorization of the expiring USA PATRIOT Act provisions."); LIBERTY AND SECURITY IN A CHANGING WORLD, *supra* note 15 at 97, n.91 (discussing two NSA programs ended in 2009 and 2011); Reports of the Attorney General on the Use of Pen Registers and/or Trap and Trace Devices Under the Foreign Intelligence Surveillance Act, (2001–2013), *available at*
www.dni.gov/files/documents/0304/PRTT%20semi%20annual%20one-page%20reports.pdf (not identifying whether the NSA or other government entity uses the authority).

20. 28 U.S.C. § 533 (2002); 28 CFR § 0.85; FBI CYBER TASK FORCE, INFORMATION SHEET, *available at* http://www.fbi.gov/about-us/investigate/cyber/cyber-task-forces-building-alliances-to-improve-the-nations-cybersecurity-1.

21. 10 U.S.C. § 2224 (2004)

22. NATIONAL SECURITY DIRECTIVE 42, NATIONAL POLICY FOR THE SECURITY OF NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS (1990), *available at*
http://www.fas.org/irp/offdocs/nsd/nsd42 [hereafter NSD-42].

law and presidential directive for national security purposes.[23] Both agencies provide technical assistance to help private sector entities respond to cyber incidents as an extension of their various authorities.[24] The military, too, conducts a range of cyber functions pursuant to defense, law enforcement, and administrative authorities. None of these cyber activities are included in the term "cyber intelligence programs." They are, however, included in this Article's more general references to cyber functions, activities, or duties of government entities.

As may be expected from any significant disclosure of state secrets, Snowden's actions create deleterious effects in many areas. A January 2014 Pew Research Center poll reveals that forty percent of respondents approve of the NSA's programs and fifty-three percent disapprove,[25] whereas a mid-2013 survey showed a majority of respondents approving of the NSA programs.[26] U.S. technology and cloud computing companies are estimated to lose between $35 and $180 billion of overseas business annually in the coming years.[27] In 2013, Cisco reported an unprecedented decline in Chinese equipment orders, which was thought to relate to Snowden's disclosures.[28] And Cisco partly attributed an additional ten percent decline in early 2014 emerging market orders to those disclosures as well.[29] Large global companies like EMC and Facebook publicly express distrust of government entities as partners in information security and technology development.[30] AOL, Apple, Dropbox, Facebook, Google, Linkedin, Microsoft, Twitter and Yahoo have

---

23. FISMA, 42 U.S.C. § 3542(b)(2) (1983).

24. Interview with National Security Agency senior officials at Ft. Meade, Md. (Feb. 27, 2014) (stating that the NSA lacks authority to provide incident response assistance directly to private sector entities but may provide such assistance through the FBI, DHS, or other agencies that ask for their assistance) [hereinafter NSA Interview].

25. PEW RESEARCH CTR., OBAMA'S NSA SPEECH HAS LITTLE IMPACT ON SKEPTICAL PUBLIC 3 (2014), *available at* http://www.people-press.org/files/legacy-pdf/1-20-14%20NSA%20Release.pdf.

26. PEW RESEARCH CTR., FEW SEE ADEQUATE LIMITS ON NSA SURVEILLANCE PROGRAM: BUT MORE APPROVE THAN DISAPPROVE 1–2 (2013), *available at* http://www.people-press.org/files/legacy-pdf/7-26-2013%20NSA%20release.pdf.

27. DANIEL CASTRO, THE INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (2013) *available at* http://www2.itif.org/2013-cloud-computing-costs.pdf (concluding that U.S. cloud computing providers may lose between $21.5 billion and $35.0 billion over the next three years);

James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER BLOGS, Aug. 14, 2013, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (arguing that the cost to overall IT service provider revenues could be as high as $180 billion).

28. Don Clark, *Cisco CEO: 'Never Seen' Such a Falloff in Orders*, WALL ST. J., Nov. 14, 2013, at B1, *available at* http://online.wsj.com/news/articles/SB10001424052702304243904579196241425599938 (Cisco chief executive John Chambers ". . . acknowledged that recent disclosures about surveillance activities by the U.S. National Security Agency may be adding to the woes facing Cisco and other U.S. companies in China, though the effect seems to be 'fairly nominal' in other countries.").

29. Nicola Leske & Edwin Chan, *UPDATE 5-Cisco Warns of Revenue Slide as Hardware Spending Sputters*, REUTERS, Feb. 12, 2014, *available at* http://www.reuters.com/article/2014/02/13/cisco-results-idUSL2N0LH20S20140213 ("That gloomy outlook, though about in line with Wall Street expectations, marks another severe decline in sales for the former high-flying tech company, which has partly blamed its poor run on a boycott of U.S. equipment after revelations of American spying efforts globally.").

30. *E.g.* ART COVIELLO, KEYNOTE ADDRESS AT THE RSA CONFERENCE (2014), *available at* http://www.emc.com/collateral/corporation/rsa-conference-keynote-art-coviello-feburary-24-2014.pdf; POSTING OF MARK ZUCKERBERG, https://www.facebook.com/zuck/posts/10101301165605491 (last visited May 7, 2014).

created a Reform Government Surveillance coalition to advocate changes to government's cyber intelligence policies and programs.[31] And the European Union has announced its intent to minimize the U.S. role in Internet governance at upcoming conferences in Turkey and Brazil.[32] In short, Snowden's disclosures of cyber intelligence programs create significant, long-lasting challenges for both public and private entities providing cybersecurity functions and otherwise seeking to develop and use cyberspace. They also expose tensions in the way government balances policy interests, applies legal norms, and ultimately develops strategic approaches to cybersecurity and cyberspace.

It is beyond the scope of this Article to further categorize or quantify beneficial and detrimental effects of Snowden's actions. Neither does this Article attempt a counterfactual comparison of benefits and harms that might have existed or accrued if the information had not been disclosed. Assuming that such efforts were possible, they are highly likely to be ephemeral as further investigation, reporting,[33] government transparency,[34] and court decisions[35] continue to sharpen the nation's focus on points of particular legal and policy interest.

This Article draws upon the additional public awareness—however limited—that Snowden's disclosures have brought to understanding the complexity of cybersecurity issues and related social, political, and legal values in discussions of cyber legislative reform.[36] It proposes that traditional thinking about national security issues must be recast to match the most important characteristics of the cyber environment—foreign/domestic, civilian/military, federal/non-federal, public/private, and regulatory/non-regulatory dualities that exist in law and related governance structures, policies, and processes. Specifically, this Article proposes a further evolution of the understanding and conduct of national security functions to achieve national cyberspace objectives.

---

31. REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/ (last visited Mar. 14, 2014).

32. PRESS RELEASE, EUROPEAN COMMISSION, COMMISSION TO PURSUE ROLE AS HONEST BROKER IN FUTURE GLOBAL NEGOTIATIONS ON INTERNET GOVERNANCE (2014), *available at* http://europa.eu/rapid/press-release_IP-14-142_en.htm.

33. *E.g.*, *Edward Snowden*, THE GUARDIAN, http://www.theguardian.com/world/edward-snowden (last visited Apr. 11, 2014); *NSA Secrets*, THE WASHINGTON POST, http://www.washingtonpost.com/nsa-secrets (last visited Apr. 11, 2014).

34. *E.g.*, *IC on the Record*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, http://icontherecord.tumblr.com (last visited Apr. 11, 2014) ("provides immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence community," content can be sorted by topics such as 'FISA,' 'FISC,' 'Section 215,' and 'Section 702').

35. *E.g.*, Klayman v. Obama, 2013 WL 6598728 (D.D.C. 2013) (granting preliminary injunction directed toward Government's bulk collection and querying of phone record data, but staying order pending appeal) *appeal docketed*, Nos. 14-5004, 14-5005, 14-5016, 14-5017 (D.C. Cir. Jan. 9, 2014), *cert. before judgment denied*, 13-931 (U.S. Apr. 7, 2014);.American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (finding Government's bulk telephony metadata program lawful) *appeal docketed*, No. 14-42 (2d Cir. Jan. 6. 2014); Jewel v. National Sec. Agency 673 F.3d 902 (9th Cir. 2011) (finding AT&T customers have standing to bring claim for mass interception of telephone, internet, and electronic communications, and reversing and remanding to district court).

36. NSA Interview, *supra* note 24 (asserting that publicly reported information from Snowden's disclosures provides only snapshots of relevant issues, equivalent to looking through a small straw).

## II. The Cyber Administrative National Security State

The term "national security" commonly refers to issues of vital national import in a way that reflexively invokes images of military action abroad, diplomatic crises, and perhaps covert or otherwise highly secretive intelligence activities—executive branch actions that aim to preserve or secure sovereign interests.[37] In government circles, lack of clarity about the meaning of the term can invite both unintentional misunderstanding and intentional debate related to its various legal and policy definitions.[38] Both outcomes are unhelpful when considering cybersecurity issues and responsibilities.

Cyberspace presents a range of dichotomous circumstances for executive and legislative bodies to comprehend. It is at once local and global, commercial and public, proprietary and open-source, civilian and military, regulated and unregulated. As cyberspace evolves, it is increasingly likely that threat actors can remotely cause kinetic attacks, disrupt vital national systems, or diminish government response capabilities. To a significant degree, information assurance, network defense, security, and resilience of energy and other infrastructure systems, military readiness, disaster response capabilities and countless other national interests present a common set of cybersecurity concerns.

To reflect these circumstances, in this Article the term "national security" refers to any concern of vital national import that federal or sub-federal governments are empowered to address. Cyber national security concerns can exist, for example, when domestic or foreign individuals or groups steal intellectual property from private computers located in one or several states, transmit the data to a foreign government, sell it to a domestic terrorist group, use the information to undermine the security or stability of U.S. energy systems or other infrastructure, extort the information owners, sell the data to criminal enterprises, or transmit the data back into the United States and create 3-D printings of equipment. Many state and federal regulatory entities have interests in these issues. The activities invite law enforcement investigations by state and federal agencies under many criminal and civil laws. Information assurance and network defense functions of private companies, state governments, and federal governments are all concerned with preventing some range of these events, identifying and disrupting ongoing actions, and responding to and recovering from emergencies. Federal and state emergency management agencies are similarly motivated to prepare for, respond to, and

37. For an expansive and thoughtful treatment of the meaning and implications of the term, see JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES, 13–22 (2007).

38. *Compare* Classified Information Procedures Act, 18 U.S.C. app. 3 § 1(b) (2012) ("'national security,' as used in this Act, means the national defense and foreign relations of the United States"), *with* THE WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE 1: ORGANIZING OF THE NATIONAL SECURITY COUNCIL SYSTEM (2009), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-1.pdf (directing the National Security Council to assist the President in "integrating all aspects of national security policy as it affects the United States – domestic, foreign, military, intelligence, and economic," as well as "international economic issues," "homeland security or counter-terrorism related issues," and "science and technology related issues"), *and* THE WHITE HOUSE, NATIONAL SECURITY STRATEGY (2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf ("We are now moving beyond traditional distinctions between homeland and national security.").

recover from natural or man-made disasters prompted by a cyber threat or involving cyber consequences for the public. The need to consider how federal and state governments can best understand and address their respective concerns is therefore compelling.[39]

This Article focuses on federal functions that address cyber national security threats during any emergency or non-emergency periods. The term "cyber administrative national security state" is used as shorthand for the collective federal executive and legislative branch entities with responsibility for cyber national security threats. This phrasing accomplishes two objectives. First, it encourages an inclusive conception of the myriad elements of federal government that must be able to operate in concert—however discordantly, fruitfully, or democratically—to address emergent cyber concerns. Second, the term conveys the highly regulated, process-driven, inter-branch nature of government's approach to cyber national security threats by calling to mind the structured regimes and processes of the administrative state. That is, the term helps conceptualize how legal, political, and social norms are incorporated into government structures and processes across military, intelligence, law enforcement, administrative, emergency response, and other cyber communities regardless whether the nation is actively facing an emergency related to military, terrorist, natural, or other threats.

The cyber administrative national security state is collectively concerned with diverse threats posed by individuals, groups, and nation-states. Attacks with kinetic effects—e.g., armed attacks, weapons of mass destruction, and acts of sabotage—are vital concerns, and they are no longer the preserve of military or intelligence arms of national governments. The cyber administrative national security state is also concerned with energy, banking, finance, health, economic, climate, and many other fields that can present vital threats. A complete listing of component entities is beyond the scope of this Article, but the NSA, U.S. Cyber Command, FBI Cyber Division, many parts of the U.S. intelligence community,[40] the DHS Office of Cybersecurity and Communications, and the Justice Department's National Security Division are among the more prominent elements of the cyber administrative national security state. Congress's committees and subcommittees with jurisdiction over these entities are the legislative branch components of the cyber administrative national security state.

## III. Cybersecurity and the Emergency Paradigm

The cyber administrative national security state is built upon and operated through a wide range of laws, policies, and processes that govern federal actions during periods of emergency and normalcy. The law applicable during emergencies includes explicit and implicit principles of emergency power rooted in the

39. *See generally* Michael J. Glennon, *State-level Cybersecurity*, 171 POL'Y REV. 85 (2012) (proposing how state governments can play important cybersecurity roles where international and federal efforts have been presumed to be primary or exclusive actors).

40. 50 U.S.C. § 3003(4) (2012); OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, http://www.intelligence.gov/mission/member-agencies.html (last visited May 7, 2014).

Constitution, legislation, court opinions, legal theory and other sources. This Article uses the term "emergency paradigm" to refer to this collective body of law. It serves as a framework to assess government's posture to address cyber national security threats in three areas: what elements of government are responsible; how are government actions regulated; and how is accountability achieved?

The Constitution's explicit foreign affairs and defense provisions serve as the organic, historical core of the emergency paradigm. Congress's duties include declaring war, raising and supporting armies, providing and maintaining a navy, governing the militia, and providing advice and consent on treaties.[41] The President's duties include making treaties, serving as commander in chief of the army and navy, and, when called into federal service, commanding the state militias.[42] The suspension of the privilege of the writ of habeas corpus "when in Cases of Rebellion or Invasion the public Safety may require it" is another element of the emergency paradigm.[43] These explicit constitutional statements are merely starting points to consider government's appropriate roles, structures, and processes to address emergency and non-emergency circumstances. The remainder of Part III describes how courts, legal theory, and framework legislation have influenced the evolution of constitutional norms and expansion of the emergency paradigm to include the broader concerns of the cyber administrative national security state.

### A. Constitutional Norms

Over the last century, two world wars, the threat of nuclear annihilation, several protected armed conflicts in Asia, hostage crises on land and sea, peacekeeping and stability efforts, global economic crises, foreign and domestic terrorist attacks on U.S. interests, and other geopolitical concerns have reshaped the emergency paradigm beyond the Constitution's explicit terms. The variety of emergency threats the nation has faced is reflected in various court decisions and legal theories about government's emergency powers. This section discusses two particularly significant influences that have placed domestic and non-military government functions at the center of the emergency paradigm and the functioning of the cyber administrative national security state.'

#### 1. *Youngstown* and Legislative Clarity

Few court cases provide broadly applicable instruction on constitutional emergency powers. One that has stood the test of time and warranted mention by courts in a range of emergency circumstances over sixty years is *Youngstown Sheet & Tube Co. v. Sawyer*.[44] The case presented the opportunity for the Supreme Court to review President Truman's executive order for the Department of Commerce to

41. U.S. CONST., art. I, § 8; *Id.* art. II, § 2.
42. *Id.* art. II, § 2.
43. *Id.* art. I, § 9.
44. 343 U.S. 579 (1952).

take possession of and operate privately owned steel mills in order to maintain steel production in the face of a threatened labor strike.[45]

Justice Hugo Black summarized a number of key facts in the Court's brief opinion: military forces were engaged in combat in Korea; Congress had passed two laws that provided mechanisms to resolve labor disputes; and Congress had considered and rejected a legislative proposal to allow the kind of emergency seizure the President directed.[46] The Supreme Court declared the President's actions unconstitutional; he had exceeded his military duties as commander in chief[47] and acted as a legislator, a function that was reserved for Congress.[48] Justice Black focused on the Constitution's overarching charges. Regarding the President's roles he wrote:

> In the framework of our Constitution, the President's power to see that the laws are faithfully executed refutes the idea that he is to be a lawmaker. The Constitution limits his functions in the lawmaking process to the recommending of laws he thinks wise and the vetoing of laws he thinks bad.[49]

And, with respect to Congress,

> the Constitution is neither silent nor equivocal about who shall make laws which the President is to execute. The first section of the first article says that "All legislative Powers herein granted shall be vested in a Congress of the United States * * *." After granting many powers to the Congress, Article I goes on to provide that Congress may "make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."[50]

In his concurring opinion, Justice Robert Jackson emphasized that Congress's duties in such circumstances did not end with declaring war, raising and equipping military forces, and making rules to regulate the military.[51] Congress alone was responsible for raising and appropriating revenue and addressing labor issues affecting industry.[52] Congress had drawn upon its several explicit constitutional duties that operate equally in emergency and non-emergency situations; President Truman's actions were unconstitutional because they did not respect the full

45. Exec. Order No. 10,340, 17 Fed. Reg. 3139 (Apr. 8, 1952).
46. 343 U.S. at 585–86.
47. *Id.* at 587.
48. *Id.* at 587-88.
49. *Id.* at 587.
50. *Id.* at 587-88.
51. *Id.* at 642-44.
52. *Id.* at 643.

complement of those duties.

*Youngstown* gives some further shape to the President's constitutional obligation to "take care that the laws be faithfully executed."[53] But the cybersecurity realm presents perhaps the ultimate tangle of circumstances that invoke the broad range of legislative duties for the executive to respect during emergencies. Congress plainly has constitutional responsibility to define and address cybersecurity needs pursuant to its exclusive legislative function, the "necessary and proper" clause, its military responsibilities, and its revenue responsibilities. Whether legislative actions in these areas speak cogently, harmoniously, or clearly on emergency actions that government might take toward the private sector or individuals becomes central to determining the lawfulness of the executive's cyber functions.

Implementing *Youngstown* in the cyber arena becomes an exercise in parsing legislative mandates related to information assurance, the use of military forces for foreign and domestic functions, cyber communications, and perhaps numerous other topics depending on the kind of cyber threat the executive faces. If the executive seeks to engage the private sector to prepare for or respond to a cyber emergency, including seizure of private property or control of industrial production within the United States, the interplay of at least four statutes must be considered from the information assurance perspective alone to discern congressional intent.

The first provides for a military-centric "Defense Information Assurance Program" through the National Defense Authorization Act for Fiscal Year 2000.[54] This law acknowledges the critical relationship between military and private systems by requiring the Secretary of Defense to coordinate with "representatives of those national critical information infrastructure systems that are essential to the operations of the Department and the armed forces on information assurance measures necessary to the protection of these systems."[55] But it does not address government seizure of private facilities or control of industrial production.

The second and third statutes both address information assurance functions operating across government agencies. The Federal Information Security Management Act of 2002 (FISMA) established general information security risk management requirements across a large number of agencies and government information systems. It tasks agency heads to provide "information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of" agency information and information systems.[56] Agencies' information security programs must take into account information systems of government contractors that handle government information. But the law does not specify whether the agencies can take any extraordinary action to protect government information on those systems during emergency circumstances.[57]

---

53. U.S. CONST. art. II, § 3.

54. Pub. L. No. 106-65, 113 Stat. 512 (1999) (codified in part in scattered titles and sections of U.S.C.).

55. 10 U.S.C. § 2224(d) (2004).

56. 44 U.S.C. § 3544(a)(1)(A) (2002).

57. *Id.* § 3544(a)(1)(A)(ii).

The third statute, the Homeland Security Act of 2002 (Homeland Security Act), presents a disjointed approach to cyber functions, responsibilities, and coordination. DHS's information security responsibilities for the federal government are most clearly identified in the 2002 transfer of the General Services Administration's Federal Computer Incident Response Center to DHS.[58] That center was established by FISMA to provide other agencies with a single federal resource for technical assistance, analysis of information security threats, information about information security threats, and consultations regarding information security and related matters.[59] But the Homeland Security Act specifies no emergency power for this operational cybersecurity entity to protect government information on government contractors' networks.

Neither does the Homeland Security Act provide such authority in a provision specifically defining the DHS role for "Enhancement of non-Federal Cybersecurity."[60] During various emergency and non-emergency periods, the department may provide "technical assistance," "analysis and warnings," and "crisis management support" to the private sector as well as state and local governments. The law does not authorize federal officials to seize or control cyber facilities or equipment or to control private production capabilities. Indeed, the private sector must request DHS cyber assistance in any of those circumstances.[61]

To the extent that Congress has directly addressed the issue of government seizure of facilities or production capabilities related to cyber emergencies, it may be in a fourth statute–the Communications Act of 1934.[62] Section 706 of that law, titled "War powers of President," defines extraordinary actions the President can take during various emergency periods even absent a declaration of war.[63] In 1951 Congress amended the law to explicitly state a presidential prerogative to suspend or amend certain Federal Communications Commission rules and regulations, close certain regulated communications stations and devices, remove communications equipment from those stations, or "authorize the use of control of any such station or device and/or its apparatus and equipment, by any department of the Government under such regulations as he may prescribe upon just compensation to the owners."[64]

Taken together, these four statutes might be interpreted to permit a range of government action to protect private sector systems or seize or control them during emergencies. However, there is significant legal and political peril for any President in such a predicament since the DOD and DHS information assurance authority falls short of allowing for such action when describing government's relationship with the private sector. Such an outcome can lead the executive to consider other plausible approaches by elements of the cyber administrative national security state

58. 6 U.S.C. § 121(g)(5) (2010).

59. 44 U.S.C. § 3546(a)(1)-(4) (2002).

60. 6 U.S.C. § 143 (2007).

61. *Id.* § 143(1), (2).

62. Pub. L. No. 73-416, ch. 652, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C. (2012)).

63. 47 U.S.C. § 606 (1984).

64. *Id.* § 606(c).

where legal authority is clearer, Congress can be engaged more efficiently, or policy can be developed in smaller circles.

The complexity that pervades government cybersecurity law and policy interests serves as background to explore Justice Jackson's further *Youngstown* commentary on the interaction of executive and legislative duties.

> We should not use this occasion to circumscribe, much less to contract, the lawful role of the President as Commander-in-Chief. I should indulge the widest latitude of interpretation to sustain his exclusive function to command the instruments of national force, at least when turned against the outside world for the security of our society. But, when it is turned inward, not because of rebellion but because of a lawful economic struggle between industry and labor, it should have no such indulgence. His command power is not such an absolute as might be implied from that office in a militaristic system but is subject to limitations consistent with a constitutional Republic whose law and policy-making breach is a representative Congress. The purpose of lodging dual titles in one man was to insure that the civilian would control the military, not to enable the military to subordinate the presidential office. No penance would ever expiate the sin against free government of holding that a President can escape control of executive powers by law through assuming his military role. What the power of command may include I do not try to envision, but I think it is not a military prerogative, without support of law, to seize persons or property because they are important or even essential for the military and naval establishment.[65]

The two divisions that helped Justice Jackson conclude that the President transgressed the Constitution are no longer so clear in cyberspace. Foreign cyber threats necessitating "instruments of national force" can operate as much within U.S. borders as throughout the "outside world." And "important or even essential" linkages between domestic industries and the global "military and naval establishment" have arguably developed into existential dependencies. This point is clarified by thinking of the military's domestic and foreign interests in secure and reliable supply chains, electricity, and other support services that operate through cyber systems to sustain garrisoned or deployed forces.

It should be readily apparent that the domestic-foreign, public-private, and military-civilian constitutional tensions presented in *Youngstown* make legislating in the cybersecurity arena challenging well beyond the concerns of seizing communications property, controlling domestic communications functions, and sustaining the military. Energy and transportation infrastructure, financial services, interstate and intrastate commerce, and federal and state government networks may all be desirable cyber targets. The President's military powers are simply a starting

65. *Youngstown*, 343 U.S. at 645–46.

point to consider steps that the cyber administrative national security state must take to understand and address security issues of the digital age.

Thus, *Youngstown*'s contribution to the emergency paradigm is twofold. First, it provides that Congress's legislative role is particularly important where the executive has no exclusive functions. Second, clarity is essential to giving effect to legislative acts. In Justice Jackson's words, "We may say that the power to legislate for emergencies belongs in the hands of Congress, but only Congress itself can prevent power from slipping through its fingers."[66] Where Congress is inactive or ambiguous, the executive is particularly reliant on theories of executive power.

2. Cybersecurity and Legal Relativism

Theoretical frameworks to understand constitutional national security powers can helpfully focus attention on points of specific legal, political, and social concern. Professor Jules Lobel has noted the decline of liberalism and the ascendency of relativism in government's approach to emergency circumstances over the past century.[67] He described the liberal view as attempting "to address the tension between law and necessity by demarcating separate spheres of emergency versus non-emergency governance."[68] The Constitution provides a base of power for an executive official to respond to an emergency, even to the point of violating the law; however, the actions are unlawful unless a court, legislature, or the populace as a whole determine otherwise.[69] In contrast, the relativist view holds that "the Constitution is a flexible document that permits the President to take whatever measures are necessary in crisis situations."[70] That is, the Constitution provides both a source of power and legal authority for executive actions taken to respond to emergencies.

Writing in 1989, Lobel observed that several factors accounted for the century-long move toward relativism regarding emergency powers.

> The routinization of crises, the rise of inherent executive power, the delegation of vast emergency power, and the sway of legal realism in the courts combined to break down the dichotomies upon which the liberal constitutional tradition was premised. Although a grey area has always accompanied the fixed dividing line between emergency and normalcy, the hazy middle zone has expanded to include most important executive exercises of foreign affairs power, resulting in broad, virtually unchecked presidential power.[71]

66. *Id.* at 654.

67. Jules Lobel, *Emergency Power and the Decline of Liberalism*, 98 YALE L.J. 1385, 1392 (1989).

68. *Id.* at 1389.

69. See *id.* at 1392–94 for a discussion of courts and legislatures responding to assertions of extra-legal necessity by military and civilian federal officers.

70. *Id.* at 1388.

71. *Id.* at 1412.

These factors are as evident today as twenty-five years ago. And the legal realist view that Lobel identified in *Youngstown* and many other court cases particularly continues to hold sway: legal norms vary according to legislative prescriptions, historical context, and other circumstances.[72]

Lobel's concern for the emergence of a larger, "hazy middle zone" where emergency powers are exercised routinely and contemporaneously with non-emergency powers remains the central emergency-power concern of the digital age. What has changed since 1989 is the emergence of cyberspace and, notably, the concern that any motivated, resourced global actor can cause a kinetic attack, stock exchange take-down, local infrastructure emergency, or other significant harm in nanoseconds.[73] State governments, the military, civilian federal agencies, and all levels of law enforcement share common concerns in this reality even before considering their unique or overlapping government functions. To further define today's emergency paradigm, the middle zone of Lobel's conceptual emergency paradigm must allow room to embrace these actors, functions, and interests. This presents the opportunity to reconsider the assignment of cyber roles across the cyber administrative national security state, mechanisms to regulate those roles, and methods and measures of accountability.

Notwithstanding the historical trend toward the relativist view of executive emergency powers, traces of liberal constitutionalism in developing cyber intelligence programs are evident in Republican and Democratic administrations alike since 9/11. Executive branch efforts to brief Congress's intelligence committees, make certain information available to all Members of Congress for review, and obtain legislative reauthorization for cyber intelligence programs ultimately seek to resolve legal, social, and political tensions in the exercise of terrorism-related emergency powers.[74] And as the Obama Administration has asserted: the FISA Court has performed its statutory role reviewing government legal arguments and authorizing emergency data collections; the government has corrected errors implementing the court's orders; and those conducting the cyber intelligence programs are governed by an array of administrative requirements that balance the constitutional issues involved.[75] Many congressional voices, including the chairmen of the House and Senate intelligence committees, have echoed this view.[76] The assertion is that the cyber administrative national security state is thus

---

72. *Id.* at 1409-11.

73. William J. Lynn, III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFFAIRS, Sept.–Oct. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

74. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT, 17–19 (2013), *available at* www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB436/docs/EBB-115.pdf.

75. *See Id.*

76. *See, e.g., Meet the Press: Intel Leaders Back President's Privacy Plan* (NBC News television broadcast Jan. 19, 2014) (transcript on file with the author), *available at* http://www.nbcnews.com/id/54117257/ns/meet_the_press-transcripts/t/january-diane-feinstein-mike-rogres-alexis-ohanian-john-wisniewski-rudy-giuliani-robert-gates-newt-gingrich-andrea-mithcell-harold-ford-#.U2vFhSgs0TA) (Mike Rogers, Chairman, House Permanent Select Committee on Intelligence, applauding and agreeing with President Obama "standing up and saying 'Hey, the [NSA] program did not have abuses. This wasn't sinister. It wasn't a rogue agency. It was legal and proper.'"); Dianne Feinstein, *The NSA's*

complying with the requirements of the emergency paradigm and thereby appropriately addressing the emergency circumstances.

These examples demonstrate only a modest nod to liberal constitutionalism as it operated into the twentieth century. Abraham Lincoln's May 1861 public order suspending the privilege of the writ of habeas corpus demonstrates that public awareness of both the constitutional emergency and the broader emergency circumstances is an important element of liberal constitutionalism. The constitutional emergency arose from the perceived ambiguity in Article I about the need for legislative action to suspend the privilege. That emergency was exacerbated when a federal court in Maryland rejected both Lincoln's order and the power of a military officer acting under it.[77] The constitutional emergency was assuaged over time through various political processes that engaged the public and Congress to find equilibrium among legal, political, and social norms for government functions, regulatory mechanisms, and accountability measures during the wartime emergency. With the Habeas Corpus Act of 1863 Congress ultimately brought a degree of resolution to the constitutional emergency by delineating broad presidential emergency authority on the issue: ". . . during the present rebellion, the President of the United States, whenever, in his judgment, the public safety may require it, is authorized to suspend the privilege of the writ of habeas corpus in any case throughout the United States, or any part thereof."[78]

In contrast to the way that the public experienced Civil War threats and related emergency powers, today's public remains at a great distance from perceiving the threats and related emergency powers of terrorism and cyber actors. Indeed, the secrecy that places government counterterrorism efforts and cyber intelligence programs beyond the public's personal experience places a unique burden on a representative government to strike appropriate balances on the public's behalf. And there is concern among scholars like Professor Andrew Bacevich that the public increasingly displays a growing fascination for militarism and technological solutions that propels government to apply military force to achieve national objectives rather than applying political pressure to curb emergencies and seek other means to achieve national security goals.[79] All of this challenges the argument that minimal public debate and limited executive branch engagement with small groups of legislators on cyber intelligence programs and related cybersecurity objectives can achieve suitable democratic outcomes.

Although the cyber administrative national security state may take significant steps to comply with and clarify the dictates of the emergency paradigm, constitutional emergencies related to cyber intelligence programs or other government cyber functions may lurk in any number of legislative or executive

---

*Watchfulness Protects America*, WALL ST. J., Oct. 13, 2013, http://online.wsj.com/news/articles/SB10001424052702304520704579125950862794052 ("The NSA call-records program is working and contributing to our safety. It is legal and it is subject to strict oversight and thorough judicial review").

77. Ex parte Merryman, 17 F. Cas. 144 (C.C.D. Md. 1861).

78. The Habeas Corpus Act, 12 Stat. 755 (1863).

79. ANDREW J. BACEVICH, THE NEW AMERICAN MILITARISM: HOW AMERICANS ARE SEDUCED BY WAR 9–33 (2005).

functions. Constitutional claims in active litigation against the executive assert First, Fourth, and Fifth Amendment concerns.[80] And upon close, public examination of the statutory and procedural recesses of the emergency paradigm, additional constitutional concerns may also appear. For example, legal arguments and interpretations of the Constitution, FISA, and other applicable law advanced for counterterrorism or other emergency needs may skew the cyber administrative national security state toward narrow understandings of the law and a narrow range of policy and legislative options to address any range of present, future, emergency, or non-emergency cyber issues.

To be clear, the revelation of any constitutional emergency through court cases or other opportunities for public scrutiny need not be viewed presumptively as willful executive transgression of clearly established norms. Congress, itself, may be the deficient constitutional actor in failing to legislate for or oversee executive functions attendant to the emergency circumstances. One dimension of this concern relates to the executive inefficiency and policy development challenges that extend from legislative ambiguity, burdensome or ineffective committee structures, or parochial procedural rules. As important to consider, however, is Congress's ability to order and operate itself to match the challenges of emergent cyber concerns. These concerns encourage an examination of the structures and processes by which the legislative and executive elements of the cyber administrative national security state operate on the continuum from non-emergency through emergency national needs.

## B. Framework Legislation

The emergency paradigm is defined and shaped as much by legislation and practice as by legal theory and courts. Framework legislation often establishes the organizational structure and processes for government entities to operate as much as it provides general authority for agency operations. In this way it carries constitutional and other legal and social norms into day-to-day government activities. The Judiciary Act of 1789, for example, ordered the judicial system.[81] And a spate of 20th century framework legislation has addressed everything from civil rights[82] and administrative procedure[83] to emergency powers,[84] disaster response,[85] and foreign intelligence.[86] As the digital age continues to see rapid

80. *See, e.g.*, Klayman v. Obama, 2013 WL 6598728 (D.D.C. Dec. 16, 2013) (alleging First, Fourth, and Fifth Amendment violations); A.C.L.U. v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (alleging First and Fourth Amendment violations); Jewel v. N.S.A., 673 F. 3d 902 (9th Cir. 2011) (alleging First and Fourth Amendment violations).

81. The Judiciary Act of 1789, 1 Stat. 73 (1789).

82. Civil Rights Act of 1964, Pub. L. No. 88-352, § 705, 78 Stat. 258 (codified as amended at 42 U.S.C. § 2000e-4 (2012)).

83. Administrative Procedure Act of 1946, Pub. L. No. 79-404, 60 Stat. 237 (codified as amended in scattered sections of 5 U.S.C.).

84. National Emergencies Act, Pub. L. No. 94-412, 90 Stat. 1255-58 (codified at 50 U.S.C. §§ 1601–1651 (2006)).

85. Robert T. Stafford Disaster Relief and Emergency Assistance Act of 1974, Pub. L. No. 93–288, 88 Stat. 143 (codified as amended at 42 U.S.C. §§ 5121-5207 (2012).

expansion, diversification, and personalized use of interconnected networks and devices,[87] framework legislation for cyberspace issues could provide a means to address increasingly complex questions of cyber policy and law in longstanding, new, large, small, technical, operational, and other parts of the cyber administrative national security state alike.

1. The "National Security Constitution" and the "Emergency Constitution"

With respect to foreign affairs functions, Professor Harold Koh has introduced the concept of the "national security constitution" to demonstrate how framework legislation, court decisions, and other sources of legal principles collectively operate in practice to shape constitutional norms.[88] The term embraces the many interrelated duties that can be discerned between the executive and legislative branches in a given foreign affairs emergency. This framing helpfully demonstrates how constitutional text, legislative intent, judicial perspectives, legal theory, and policy interests come together to shape government action. The concept is equally applicable to the broader range of cyber national security concerns of the emergency paradigm.

Professor Bruce Ackerman has proposed another concept related to constitutional norms and framework legislation that enables thoughtful analysis of cybersecurity issues. Writing after 9/11 he advocated new framework legislation continuing the aims of the National Emergencies Act of 1976 to improve government's functioning during terrorist-related emergencies.[89] Concerns about unwarranted detention and lack of access to civilian courts contributed to his proposal to reconstitute an "emergency constitution" through framework legislation that would improve the balance between security needs and individual liberties. He recommended supermajority voting requirements to continue any presidentially declared emergency,[90] broader access to executive branch information for majority and minority parties in Congress,[91] financial compensation to victims of preventive detention,[92] and new norms for judges to apply during emergency periods.[93] The hope was to avoid historical failures like the Japanese-American internment camps of World War II.[94] Lest these concerns about using military forces domestically to respond to national security threats be considered an anachronism, cyber- and

86. FISA, *supra* note 12.

87. *See, e.g.*, Jonathan Zittrain, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008); Jack Goldsmith & Timothy Wu, WHO CONTROLS THE INTERNET?: ILLUSIONS OF A BORDERLESS WORLD (2006); Julie Cohen, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012).

88. Harold Hongju Koh, *Why the President (Almost) Always Wins in Foreign Affairs: Lessons of the Iran-Contra Affair*, 97 YALE L.J. 1255, 1282–84 (1988).

89. Bruce Ackerman, *The Emergency Constitution*, 113 YALE L. J. 1029, 1031–32 (2004).

90. *Id.* at 1047–49.

91. *Id.* at 1050–53.

92. *Id.* at 1062–66.

93. *Id.* at 1066–74 (proposing that judges' overriding concern be decency with respect to torture, detention, and other emergency concerns).

94. *See id.* at 1041–45.

terrorism-related debates should be informed by the knowledge that in 2002 the Bush Administration considered using military forces to detain five terrorism suspects near Buffalo, New York.[95]

Ackerman's emergency constitution continues a tradition of scholarly focus on legislative solutions to the challenges of executive excess, preservation of civil liberties, increased transparency, and effective oversight.[96] It proposes that a return to liberal constitutionalism is both possible and valuable, at least to improve the nation's approaches to terrorist-related emergencies. Considering the new threat landscape that military and intelligence communities face carrying out counterterrorism operations like the raid that killed Osama bin Laden, Professor Robert Chesney has also recommended updates to framework legislation to improve information sharing with Congress, promote executive branch accountability for military and intelligence operations, and provide clear legal authority for the conduct of military cyber actions according to international and federal law.[97] While scholarly calls for legislative solutions are by no means exclusive,[98] the common theme is that the legislative process returns benefits that cannot otherwise be achieved.

2. Framework Legislation for the Emergency Paradigm

*Military and Intelligence Reform*

Many framework statutes establish structures and processes for the cyber administrative national security state. Defense, foreign affairs, and intelligence functions were first treated comprehensively in the National Security Act of 1947 (National Security Act),[99] which continues to serve as a cornerstone of the emergency paradigm. The National Security Act recast the post-war military and intelligence enterprise to improve executive branch organizational structures and policy coordination mechanisms in three significant ways.[100] The first was the establishment of a National Security Council (NSC)

> to advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security so as to enable the military services and the other departments and agencies of the Government to cooperate more effectively in matters involving the

95. Mark Mazzetti & David Johnston, *Bush Weighed Using Military in Arrests*, N.Y. TIMES, Jul. 25, 2009, http://www.nytimes.com/2009/07/25/us/25detain.html?_r=0.

96. *See, e.g.*, Gerhard Caspar, *The Constitutional Organization of the Government*, 26 WM. & MARY L. REV. 177 (1985).

97. Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SECURITY L. & POL'Y 539, 543-44 (2012).

98. *See, e.g.*, Robert F. Blomquist, *American National Security Presiprudence*, 26 QUINNIPIAC L. REV. 439 (2008).

99. National Security Act, *supra* note 14.

100. *Id.* § 2.

national security."[101]

Second, the National Security Act created a cabinet-level secretary[102] and a Joint Chiefs of Staff[103] to provide unified management of the military services as a single entity—the "national military establishment."[104] The Secretary of Defense was charged to serve as a member of the NSC and as the "principal assistant to the President in all matters relating to the national security."[105] Finally, the National Security Act established the CIA as a function of the NSC.[106] Congress amended the National Security Act two years later to create the DOD out of the national military establishment.[107]

Since the CIA's creation, structures and processes regulating the U.S. intelligence community have evolved as much by internal executive branch prerogative as by legislative action. Notably, Executive Order 12,333 continues to provide important guidelines for the collection of intelligence and the conduct of intelligence activities, including cyber intelligence programs.[108] In creating judicial and executive branch processes to regulate the collection and use of communications for foreign intelligence purposes, the FISA of 1978 serves as a cornerstone of cyber-related framework legislation. Through Snowden's disclosures FISA is known to be the basis for significant government contacts with U.S. industry and the capability for various intelligence agencies to collect large volumes of communications data from cyberspace for counterterrorism purposes. But the framework legislation with the largest impact on the future of government's posture to address strategic cybersecurity issues from an intelligence perspective is the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[109]

IRTPA's most significant contribution to the emergency paradigm is the establishment of a Director of National Intelligence (DNI) to provide a point of coordination and leadership outside any one intelligence agency.[110] This fulfilled a longstanding objective of intelligence reform[111] and enables the strategic growth and coordination of intelligence functionalities. By amendment to the National Security Act, the DNI "act[s] as the principal adviser to the President, to the National Security Council, and the Homeland Security Council for intelligence matters related to the national security."[112] IRTPA's other significant contribution

101. *Id.* § 101(a); 50 U.S.C. § 3021(a) (2012).

102. National Security Act, *supra* note 14, § 202.

103. *Id.* § 211.

104. *Id.* § 201.

105. *Id.* §§ 101(a), 202(a).

106. *Id.* § 102(d).

107. National Security Act Amendments of 1949, ch. 412, sec. 4, § 201, 63 Stat. 578-79.

108. *Supra* note 13.

109. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified as amended in scattered sections of the U.S.C.).

110. 50 U.S.C. §§ 3023(b)(1), (c) (2004).

111. COMM'N ON THE ROLES AND CAPABILITIES OF THE U.S. INTELLIGENCE COMTY., PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE app. A-13 (1996) [hereinafter 1996 U.S. Intelligence Community Report].

112. 50 U.S.C. § 3023(b)(2) (West 2004).

is the creation of new organizations and functions to deliver a strategic, nationwide, public-private, intelligence capability.

The most significant element of this capability is the National Counterterrorism Center (NCTC), which develops operational counterterrorism plans to integrate "all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies"[113] on behalf of the DNI. Extending from these planning responsibilities, the NCTC also assigns cyber and other counterterrorism roles and responsibilities to other government agencies.[114] IRTPA supplements this federal level of intelligence activity with a nationwide, intergovernmental, public-private information sharing framework and network. Under the DNI's direction, federal, state, local, and tribal entities and the private sector collaborate to create an "Information Sharing Environment"[115] through which they develop common means to share terrorism information.[116] And reflecting the coordinated approach to intelligence that the DNI was envisioned to provide, the DNI has commissioned the FBI to lead regional intelligence centers that connect government and private entities.[117] In short, iterative changes to the FISA and the new structural regime provided by the IRTPA have reshaped the emergency paradigm to create an expansive national intelligence enterprise to address concerns related to cyber terrorism. The methods that intelligence agencies employ, the relationships they establish with the private sector and other governments, and the information they can assess enable them to perform or help perform many federal and sub-federal government cybersecurity functions beyond the concerns of cyber terrorism.

*Commercial, International, and Economic Emergencies*

Another cornerstone of the emergency paradigm is the National Emergencies Act of 1976, which provides a framework for the executive to declare and exercise emergency powers described in law by Congress.[118] The law ensures a degree of public awareness, congressional engagement, and government transparency and accountability by requiring the President to: declare an emergency publicly, identify the specific provisions of law describing the emergency powers being exercised, transmit the declaration to Congress, publish the declaration in the Federal Register, and report to Congress on emergency expenditures.[119] Congress clearly envisioned the law as a mechanism to avoid persistent states of emergency. With few

113. 50 U.S.C.A § 3056(d)(2) (West 2004).

114. *Id.*§ 3056(d)(3).

115. 6 U.S.C.A. § 485(a)(3), (b) (2010); OFFICE of the DIR. of NAT'L Intelligence, Information Sharing Environment, *available at*,http://www.dni.gov/index.php/about/organization/information-sharing-environment-who-we-are.

116. 6 U.S.C.A. § 485(a)(5).

117. Greg Miller, *FBI gets a broader role in coordinating domestic intelligence activities*, WASH POST, June 19, 2012, http://www.washingtonpost.com/world/national-security/fbi-gets-a-broader-role-in-coordinating-domestic-intelligence-activities/2012/06/19/gJQAtmupoV_story.html.

118. Pub. L. No. 94-412, 90 Stat. 1255 (1977) (codified as amended at 50 U.S.C. §§1601 *et seq.* (2000)).

119. 50 U.S.C. §§ 1521(a), 1641(c).

exceptions, upon enactment it terminated all states of emergency within two years.[120] And it required the Senate and House to meet within six months of newly declared emergencies "to consider a vote on a joint resolution to determine whether that emergency shall be terminated."[121] However, according to one recent study, Congress has never taken action under this provision,[122] and thirty ongoing states of emergency were in effect as of 2013.[123]

The International Emergency Economic Powers Act of 1977[124] reflects an attempt to establish procedures by which the executive and legislative branches interoperate when the President wishes to take emergency actions related to foreign exchange transactions, foreign property interests, foreign credit transfers or payments, or importing or exporting of currency or securities.[125] It builds upon the National Emergencies Act and requires supplemental executive consultation with and reporting to Congress.[126] The law acknowledges the President's constitutional power to take measures "to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." Many cybersecurity concerns conceivably fall within this broad language; however, Congress has further provided that the President's authority does not extend to

> (1) any postal, telegraphic, telephonic, or other personal communications, which does not involve a transfer of anything of value; . . . or
>
> (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or information materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and new wire feeds.[127]
>
> From one perspective, the law allows flexibility for Congress and the President to consider whether and how cyberspace concerns should be understood and addressed as emergencies. From another perspective, the law's ambiguity handicaps both branches in planning for the particular circumstances of the digital age.

120. *Id.* §§ 1601(a), 1651.

121. *Id.* § 1622(b).

122. Patrick A. Thronson, *Toward Comprehensive Reform of America's Emergency Law Regime*, 46 MICH. L. REV. 737, 752 (2013).

123. *Id.* at 754.

124. Pub. L. No. 95-223, §§ 201-208, 91 Stat. 1625, 1626-29 (1977) (codified as amended at 50 U.S.C. §§ 1701–1706 (2001)).

125. 50 U.S.C. § 1702(a)(1) (2001).

126. *See id.* § 1703.

127. *See id.* § 1702(b).

*Federal Emergency Preparedness, Response, and Critical Infrastructure Protection*

Framework legislation in 1970,[128] 1974,[129] and 1988[130] developed today's Federal Emergency Management Agency (FEMA) to integrate federal, state, and local government efforts for emergency preparedness, response, recovery, and disaster assistance. The present Robert T. Stafford Disaster Relief and Emergency Assistance Act enables federal planning, training, exercises, research and other capabilities for cyber emergencies primarily through its emergency preparedness provisions.[131] This covers

> all those activities and measures designed or undertaken to prepare for or minimize the effects of a hazard upon the civilian population, to deal with the immediate emergency conditions which would be created by the hazard, and to effectuate emergency repairs to, or the emergency restoration of, vital utilities and facilities destroyed or damaged by the hazard.[132]

Cyber emergencies are included here because the term "hazard" is defined to include any "man-caused event."[133]

FEMA may have broader cyber capabilities and responsibilities by virtue of its specific disaster assistance and emergency response functions related to "major disasters." This term is defined to mean any natural catastrophe or

> regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this chapter to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.[134]

Cyber threats from foreign nations, terrorist groups, or individuals may cause fires, floods or explosions through computers regulating water levels of dams, electricity-distribution systems, or other elements of publicly or privately owned, operated, maintained, regulated, or administered critical infrastructure.

Congress has linked this long-standing FEMA focus on disasters, preparedness, and emergency response to national cyber objectives and broader critical infrastructure protection interests only lightly. The Critical Infrastructures

128. Disaster Relief Act of 1970, 84 Stat. 1744, 15 U.S.C. § 636a (repealed by Pub. L. 97-35).

129. Disaster Relief Act Amendments of 1974, Pub. L. 93-288, 88 Stat. 143.

130. Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5121 (1988).

131. *See id.* § 5131.

132. *Id.* § 5195a(a)(3).

133. *See id.* § 5195a(a)(1)(b).

134. *Id.* § 5122(2).

Protection Act of 2001[135] asserted a congressional finding that a "continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States."[136] Congress further provided that:

> It is the policy of the United States
>
> (1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States;
>
> (2) that actions necessary to achieve the policy stated in paragraph (1) be carried out in a public-private partnership involving corporate and non-governmental organizations; and
>
> (3) to have in place a comprehensive and effective program to ensure the continuity of essential Federal Government functions under all circumstances.[137]

No agency roles are assigned to carry out these objectives. But a National Infrastructure Simulation and Analysis Center created by the law "to serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counterterrorism, threat assessment, and risk mitigation"[138] now operates through the DHS Office of Infrastructure Protection.[139] This office collaborates with FEMA and the private sector pursuant to 2007 amendments to the Homeland Security Act to jointly develop guidance, recommendations, best practices, and voluntary preparedness standards to address private sector interests.[140]

The most recent, collective legislative treatment of cyber, infrastructure, and emergency management issues is the 2007 reconstitution of FEMA with a primary mission to "reduce the loss of life and property and protect the Nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters

---

135. Pub. L. 107-56, § 1016, 115 Stat. 400 (codified at 42 U.S.C. § 5195c (2001)).

136. *Id.* § 5195c(b)(3).

137. *Id.* § 5195c(c).

138. *Id.* § 5195c(d)(1).

139. Department of Homeland Security Appropriations Act, 2007, § 611(13) (codified at 6 U.S.C. § 321); *see* U.S. DEPARTMENT OF HOMELAND SECURITY, "ABOUT THE NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER," *available at* http://www.dhs.gov/about-national-infrastructure-simulation-and-analysis-center.

140. Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title IX, § 901(a), Aug. 3, 2007, 121 Stat. 364 (codified at 6 U.S.C. § 321l).

by leading and supporting the Nation in a risk-based, comprehensive emergency management system of preparedness, protection, response, recovery, and mitigation."[141] More specifically, amendments to the Homeland Security Act charge the FEMA Administrator to

> coordinate the implementation of a risk-based, all-hazards strategy for preparedness that builds those common capabilities necessary to respond to natural disasters, acts of terrorism, and other man-made disasters while also building the unique capabilities necessary to respond to specific types of incidents that pose the greatest risk to our Nation. [142]

While it is clear that FEMA's preparedness and response capabilities must be available for an emergency with a cyber dimension, it remains unclear whether Congress's iterative approach to these issues is meant to go further. The language could be understood to mean that FEMA should develop cyber capabilities to actively mitigate cyber threats posed by terrorists or other threat actors so public-private risk-management programs are conducted fluidly by a single government entity from a period of normalcy through an emergency and back to normalcy. Yet these laws were contemporaneous with both the reauthorization of government's cyber intelligence programs and the further development of other DHS offices to achieve specific information security, cybersecurity and critical infrastructure objectives.

*Congressional Reform*

Congress has taken comparatively less opportunity to reconfigure its committees and redefine its chamber rules to match executive branch reforms. But congressional reform preceded legislation to reorder the executive branch during the military and intelligence reform periods of the 1940s and 1970s. The Legislative Reorganization Act of 1946 created armed services committees in each chamber to oversee and legislate for the military establishment created by the National Security Act.[143] And in 1976 and 1977, respectively, the Senate and House established the current select committees on intelligence.[144]

Reporting of intelligence activities to Congress changed markedly beginning in the 1970s. Covert CIA operations were first required to be reported to Congress in 1974 through an amendment to the Foreign Assistance Act.[145] Four years later,

141. Department of Homeland Security Appropriations Act, 2007, § 611(11), Pub. L. 109-295, 120 Stat. 1355 (codified at 6 U.S.C. § 313(b)(1)).

142. *Id.* § 314(b).

143. Legislative Reorganization Act of 1946, ch. 753, §§ 102, 121, 60 Stat. 812, 815, 822, 824.

144. 1996 U.S. Intelligence Community Report, *supra* note 111, at A-18.

145. Pub. L. No. 93-559, § 662(a), 88 Stat. 1804, *repealed by* Intelligence Authorization Act for Fiscal Year 1991, § 601. Upon repeal of the 1974 reporting requirement, Congress created a new, broader framework for oversight of intelligence activities in the National Security Act, which is codified as amended at 50 U.S.C. § 3091 *et seq.*.

FISA established semi-annual reporting requirements "concerning all electronic surveillance" within the United States for foreign intelligence purposes.[146] It also required reports of administrative procedures established by the Attorney General to minimize the acquisition, retention, and sharing of non-public information.[147] Congress has further updated executive branch reporting requirements sporadically since 1980.[148] But the structures and processes of the intelligence committees themselves, particularly following 9/11, have changed little and are viewed by government and outside groups as dysfunctional and counterproductive.[149] And a longstanding proposal for Congress to operate a joint intelligence committee modeled on the Joint Committee on Atomic Energy has never succeeded.[150] Neither have the proposals of the U.S. National Commission on Terrorist Attacks Upon the United States regarding comprehensive legislative reform to enable efficient intelligence and homeland security legislation and oversight.[151]

The hallmarks of government's recent changes to the emergency paradigm are the legislative reforms that created the new concept of homeland security and then reconstituted government to focus more specifically on long-standing counterterrorism interests. The two fields operate according to contradictory norms. Homeland security activities are characterized by open engagement across government and non-government communities to achieve broad national objectives, including counterterrorism. In contrast, policies and functions developed through intelligence entities focused on counterterrorism are characterized by secrecy and limited-access forums. While the Homeland Security Act was Congress's first attempt to provide the paradigm to integrate counterterrorism objectives with broader national strategies, the IRTPA and other laws subsequently provided separate government structures and processes. And there remains as much uncertainty in the legal frameworks that regulate agencies within each field as at the points where the two fields attempt to work together effectively.

3. Cybersecurity Law and Organization

Framework legislation does not exist for cybersecurity. Congress's trend since the 1980s has been to address digital age issues separately. The Computer Security

146. FISA, *supra* note 12, §§ 102(a), 106.

147. *Id.* §§ 107, 108.

148. *See* 1996 U.S. Intelligence Community Report, *supra* note 111, at A-19–25 (noting the Intelligence Oversight Act of 1980, the Goldwater-Nichols Department of Defense Reorganization Act of 1986, legislation in 1989 to establish an Inspector General for the CIA, and the Intelligence Authorization Act for Fiscal Year 1993).

149. L. ELAINE HALCHIN & FREDERICK M. KAISER, CONG. RESEARCH SERV., RL32525, CONGRESSIONAL OVERSIGHT OF INTELLIGENCE: CURRENT STRUCTURE AND ALTERNATIVES, Report 1–9 (2012), *available at* www.fas.org/sgp/crs/intel/RL32525.pdf (noting reports of the National Commission on Terrorist Attacks Upon the United States, Commission on Weapons of Mass Destruction, Bipartisan Policy Center, and Council on Foreign Relations).

150. *Id.*

151. THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 419-21.

Act of 1987,[152] the Communications Decency Act of 1996,[153] the Digital Millennium Copyright Act of 1998,[154] and the E-Government Act of 2002[155] speak to this norm. So does the trend to incrementally update the criminal code to address technological advances and privacy, for example, through the Computer Fraud and Abuse Act of 1986,[156] the Electronic Communications Privacy Act of 1986,[157] and the Communications Assistance to Law Enforcement Act of 1994.[158]

In the area of information security, FISMA comes closest to serving as framework legislation because it establishes a widely applicable compliance program and assigns responsibilities to specific officials within agencies and at the White House. While agency heads are responsible for implementing information security programs, the Director of the Office of Management and Budget bears overall responsibility for those programs and reporting to Congress. DOD and CIA information systems are excepted from the Director's responsibility.[159]

The Homeland Security Act places DHS's information security functions in a broader framework. DHS operates the government incident handling center for information security established by FISMA and subsequently transferred to DHS.[160] Similar expertise is available to enhance cybersecurity for the private sector and state, local, and tribal governments. And the Homeland Security Act transferred a range of cyber, communications, and related infrastructure functions from the FBI, DOD, Department of Commerce, and Department of Energy.[161] Each of these entities—the National Infrastructure Protection Center, National Communications System, Critical Infrastructure Assurance Office, and National Infrastructure Simulation and Analysis Center respectively—had relationships with the private sector.

Many functions closely related to information security remain distributed across government. The National Telecommunications and Information Administration within the Department of Commerce manages Internet governance issues.[162] The Commerce Department's National Institute of Standards and Technology establishes technical standards for civilian government information systems.[163] The NSA establishes technical standards for government information systems handling classified national security information.[164] And independent regulatory agency roles include: the Federal Communications Commission's role regulating interstate and international communications by radio, television, wire,

152. Pub. L. No. 100-235, 101 Stat. 1724.

153. Pub. L. No. 104-104, 110 Stat. 56.

154. Pub. L. No. 105-304, 112 Stat. 2860.

155. Pub. L. No. 107–347, 116 Stat. 2899.

156. Pub. L. No. 98-473, 98 Stat. 1837 (1984).

157. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 2510-2522 (2002)).

158. Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010 (1994)).

159. FISMA, 44 U.S.C. § 3543(c) (2002).

160. *Id.* § 3546.

161. Homeland Security Act of 2002, 6 U.S.C. § 121(g)(1)-(4) (2010).

162. 15 U.S.C. § 1512; 47 U.S.C. § 902(b)(2)(H); 47 U.S.C. § 901(c)(3); Exec. Order No. 12,046, 43 Fed. Reg. 13,349 (Mar. 29, 1978) (revoked in part).

163. 40 U.S.C. § 11331 (2006); 15 U.S.C. § 278g–3 (2006).

164. NSD-42, *supra* note 22.

satellite and cable;[165] the Federal Energy Regulatory Commission's role enforcing cybersecurity reliability standards across the bulk power system;[166] the Federal Trade Commission's role enforcing "unfair or deceptive acts or practices" related to cyber privacy policies and other cybersecurity concerns;[167] and the Securities and Exchange Commission's guidance that companies disclose cybersecurity risks and incidents to comply with the Securities Act of 1933 and the Securities Exchange Act of 1934.[168] Congress provides funding, oversight, and legislation in these areas through committees with primary jurisdiction for respective agencies, not through a single committee or comprehensive cyber coordination process.

Agencies have increasingly sought close coordination and even fusion of these cyber functions distributed across the executive branch. By agreement with the Director of the Office of Management and Budget, the Department of Homeland Security now performs a number of FISMA functions that complement DHS's cyber incident handling, analysis and warning, and technical assistance functions described both in FISMA and the Homeland Security Act.[169] The FBI, DHS, and NSA all operate cyber centers to integrate other government cyber interests and knowledge with their core investigative/intelligence, infrastructure protection, and military/intelligence cyber programs respectively.[170] Most significantly, government's signals intelligence, military information assurance, and cyber warfighting capabilities are fused by having the same individual lead the NSA and U.S. Cyber Command.

This dual command structure for the NSA and U.S. Cyber Command speaks to the long-standing, robust capability that exists across certain elements of the cyber administrative national security state to address cyber intelligence and defense matters. As currently constructed, U.S. Cyber Command reflects numerous evolutionary steps that the defense community has taken since the mid-1980s with armed services committees, defense appropriations committees, intelligence committees, and other elements of Congress to understand and address military and related cyber threats. The NSA has gone through similar strategic changes. In 1999 an agency review team concluded that the "NSA is an organization ripe for divestiture: its individual capabilities are of greater value than is the organization as a whole." The agency envisioned a future in which it "operates and thrives in the

165. 47 U.S.C. § 151 *et seq.* (2006).

166. Energy Policy Act of 2005, § 1211 (codified at 16 U.S.C. § 824o (2006)).

167. 15 U.S.C. § 45 (2006).

168. SEC. EXCH. COMM'N., CF DISCLOSURE GUIDANCE: TOPIC NO. 2—CYBERSECURITY (2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

169. *See, e.g.*, MEMORANDUM M-10-28 FROM THE DIRECTOR OF THE OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT TO THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (2010), *available at* http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-28.pdf;

170. FEDERAL BUREAU OF INVESTIGATION, NATIONAL CYBER INVESTIGATIVE JOINT TASK FORCE, http://www.fbi.gov/about-us/investigate/cyber/ncijtf (last visited Apr. 21, 2014); U.S. DEPARTMENT OF HOMELAND SECURITY, NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center (last visited Apr. 21, 2014); WHITE HOUSE, NATIONAL CYBERSECURITY POLICY CAPTURE, http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf (last visited Apr. 21, 2014).

net" of the digital age as part of a plan to demonstrate value to the government beyond the sum of its various parts.[171] Whether as a direct result of subsequent planning or a combination of other factors, Snowden's disclosures reveal an element of fulfillment of long-standing, strategic NSA objectives, ostensibly understood and supported by the NSA's legislative counterparts in the cyber administrative national security state. The historic core of the emergency paradigm has evolved through such close relationships, while the newer elements develop at some remove from those activities through a non-military, non-intelligence, non-law enforcement set of relationships in the cyber administrative national security state.

## IV. Conclusion

Cybersecurity has emerged as the next great test of the emergency paradigm. To date, legislation to prepare the nation for cyber emergencies has largely focused on developing military and intelligence organizations and capabilities. Assuming that some range of threats will continue to clearly warrant such treatment, Congress's focus on military and intelligence organizations and issues is not surprising. But that focus limits Congress's view of broader cyberspace issues.

Unlike previous initiatives to organize itself and then the executive branch to meet twentieth-century security challenges, Congress has been unable to address cross-cutting cyber concerns. Whereas the military threats of the Cold War necessitated an analogous response to deter or respond to attacks, the nature of cyberspace is different. Cybersecurity concerns can conceivably be precluded, mitigated, or otherwise addressed by private, sub-federal government, and civilian federal government entities. The arguments for military, intelligence, and law enforcement actors operating in relative secrecy under special legal authority are therefore to be constructed, not presumed.

In short, the cyber administrative national security state must be capable of correcting course and forming itself to embrace public, economic, trade, civil liberties, regulatory, international, and other concerns. This expansive range of issues should encourage Congress to dedicate significant effort to drafting framework legislation that extends beyond foreign intelligence issues. The need for such comprehensive treatment predates Snowden's disclosures; his actions have simply clarified and publicized certain ways in which constitutional questions arise in the digital age.

171. Nat'l Sec. Agency, NEW ENTERPRISE TEAM RECOMMENDATIONS: THE DIRECTOR'S WORK PLAN FOR CHANGE (1999), *available at* http://www.nsa.gov/public_info/_files/directors_misc/Directors_Work_Plan.pdf.