CYBERSECURITY AND EXECUTIVE POWER

DAVID W. OPDERBECK[*]

ABSTRACT

This Article analyzes the constitutional authority of the President to shut down or limit public access to the Internet in a time of national emergency. The threats posed by cybercrime, cyberwarfare, and cyberterrorism are significant. It is imperative that national governments and international policymakers develop defenses and contingency plans for such attacks. At the same time, the threats to civil liberties posed by current legislative cybersecurity proposals are equally real. Executive power to disrupt Internet access in the name of security can become as potent a weapon against democracy as a hacker's attempt to take down the power grid. This Article examines current cybersecurity proposals in Congress and explains why they are in many ways misguided. It then examines the constitutional law of presidential power against the backdrop of recent efforts by Congress and the Executive to regulate cyberspace. The Article concludes with a proposed cybersecurity policy matrix, which could help courts and policymakers manage the difficult constitutional and policy tensions raised by the problem of cybersecurity.

TABLE OF CONTENTS

∗ Professor of Law, Seton Hall University Law School. Thanks to Derek Bambauer, Eric Goldman, and the participants in the Santa Clara Internet Law workshop for valuable comments on earlier drafts. Thanks also to Stephanie Backes for excellent research assistance.

I. INTRODUCTION

In January and February 2011, an extraordinary wave of popular revolt swept through parts of North Africa.[1] Citizens in Tunisia and Egypt, who had been dominated by autocratic governments for decades, overthrew their rulers, including long-time Egyptian president Hosni Mubarak.[2] Some called the events in Egypt a "Facebook Revolution," symbolized by its youthful leaders, such as Google executive Wael Ghonim.[3] The Internet and social networks facilitated a degree of coordination and courage among ordinary people that would have been unthinkable less than a decade ago. Ghonim, who was imprisoned for twelve days before Mubarak's fall for helping organize protests through Facebook, exuberantly stated after Mubarak resigned, "This revolution started on

1. *See, e.g.*, *The Upheaval in Egypt: An End or a Beginning?*, ECONOMIST, Feb. 5, 2011, at 35, *available at* http://www.economist.com/node/18063746?story_id=18063746.

2. *See, e.g.*, *Egypt After Mubarak: Where Now for Egypt and the Region?*, ECONOMIST (Feb. 15, 2011, 5:21 PM), http://www.economist.com/blogs/newsbook/2011/02/egypt_after_mubarak.

3. *See, e.g.*, Catharine Smith, *Egypt's Facebook Revolution: Wael Ghonim Thanks the Social Network*, HUFFINGTON POST (Feb. 11, 2011, 3:36 PM), http://www.huffingtonpost.com/2011/02/11/egypt-facebook-revolution-wael-ghonim_n_822078.html; *see also After Mubarak: The Autumn of the Patriarchs*, ECONOMIST, Feb. 19, 2011, at 29, *available at* http://www.economist.com/node/18186984?story_id=18186984.

Facebook. This revolution started . . . in June 2010 when hundreds of thousands of Egyptians started collaborating content."[4]

In fact, cyberspace was in many ways the front line of the Egyptian revolution. Although Mubarak apparently lacked the support among the Egyptian military for sustained attacks on civilians, he waged a desperate last-gasp battle to shut down access to the Internet so that organizers could not effectively communicate with each other, the public, or the outside world.[5]

Could a similar battle over cyberspace be waged in developed democracies, such as the United States? Policymakers in the West are justifiably concerned about cyberattacks, cyberterrorism, and the possibility of cyberwar. The raging question is whether a democratic state governed by constitutional principles and committed to free speech and private property rights can promote cybersecurity without destroying the Internet's unique capacity to foster civil liberties.

Cyberspace is as vulnerable as it is vital. The threat is real. President Obama recently declared that "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[6] Cybersecurity has been described as "a major national security problem for the United States."[7] Private and public cyber-infrastructure in the United States falls under nearly constant attack, often from shadowy sources connected to terrorist groups, organized crime syndicates, or foreign governments.[8] These attacks bear the potential to disrupt not only e-mail and other online communications networks, but also the national energy grid, military-defense ground and satellite facilities, transportation systems, financial markets, and other essential

4. Smith, *supra* note 3.

5. *See, e.g.*, *Internet Blackouts: Reaching for the Kill Switch*, ECONOMIST, Feb. 12, 2011, at 58, *available at* http://www.economist.com/node/18112043?story_id=18112043. Whether this revolution will prove stable over the long term, of course, remains a live and difficult question. *See, e.g.*, *Egypt's Turmoil: It Goes On and On*, THE ECONOMIST, Feb. 11, 2012, http://www.economist.com/node/21547294.

6. President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure (May 29, 2009), *available at* http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure.

7. CTR. FOR STRATEGIC & INT'L STUDIES, SECURING CYBERSPACE FOR THE 44TH PRESIDENCY 1 (2008) [hereinafter CSIS REPORT], *available at* http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

8. *See infra* Part II.

facilities.[9] In short, a substantial cyberattack could take down the nation's entire security and economic infrastructure.[10]

U.S. policymakers are justifiably concerned by this threat. Existing U.S. law is not equipped to handle the problem. The United States currently relies on a patchwork of laws and regulations designed primarily to address the "computer crime" of a decade ago, as well as controversial antiterrorism legislation passed after the September 11 attacks, and some general (and equally controversial) principles of executive power in times of emergency.

Current proposals for containing the threat, however, could significantly increase U.S. government power—particularly presidential power—over the Internet. An influential report that informs current U.S. policy bluntly offers this remedy for holes in cybersecurity: "Regulate cyberspace."[11] According to the report, "[t]he United States must . . . set minimum standards for securing cyberspace in order to ensure that the delivery of critical services in cyberspace continues if the United States is attacked."[12]

This broad regulatory approach was reflected in a bill introduced in the Senate, the "Cybersecurity Act of 2009."[13] The Cybersecurity Act's most controversial provision was a grant of authority to the President to "declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network."[14] In short, the President would have been authorized to shut down cyberspace, or at least the portion of cyberspace that interfaces with the United States.

Cyber civil libertarians reacted to this proposal with swift anger. No threat, they argued, justifies empowering the President with an Internet "kill switch."[15] In response to these complaints, more recently proposed

---

9. *See infra* Part II.

10. *See infra* Part II. Some commentators, however, argue that the claimed threats are exaggerated and that the Internet is inherently self-healing. *See* Derek E. Bambauer, *Conundrum*, 96 MINN. L. REV. 584, 616–21 (2011). Professor Bambauer would focus cybersecurity regulation on mandating data redundancy. *Id.* at 643–53. Data redundancy is certainly good policy in general, although making multiple copies of sensitive data means that there are multiple avenues through which that data can be stolen. But at least two questions remain: given redundant systems, what would constitute an "emergency"; and what authority, if any, should the President have in case of such an event?

11. CSIS REPORT, *supra* note 7, at 2.

12. *Id.*

13. S. 773, 111th Cong. (as introduced, Apr. 1, 2009).

14. *Id.* § 18(2).

15. *See, e.g.*, Jon Swartz, *Should the Internet Have an 'Off' Switch?*, USA TODAY, Feb. 16, 2011, at 1B.

legislation softens the kill switch language.[16] Nevertheless, it appears that the President could retain the power to "disconnect" compromised portions of the Internet without the need for any prior judicial review.

Cybersecurity policy thus raises fascinating and difficult questions about regulatory design, executive power, and jurisdiction over "cyberspace." This Article examines the President's ability to exert emergency control over cyberspace under U.S. law. Part II describes some serious threats to cybersecurity, including the practice of cyberwar, and surveys existing law and proposed legislation relating to cybersecurity. Part III examines constitutional limitations and the President's ability to control cyberspace, including in a time of cyber crisis or cyberwar. Part IV begins to develop a matrix for constructing a balanced cybersecurity policy, which is explored more fully in Part V.

II. CYBERWAR AND THE MOVE TO REGULATE CYBERSPACE

A. Cyberwarfare, Cyberterrorism, and Organized Cybercrime

Cyber is the new domain of international espionage, sabotage, and war. China, Russia, the United Kingdom, and the United States employ extensive cyber spying networks.[17] A coordinated series of denial-of-service and other attacks could cripple a state's political and communications systems, as happened during "Web War 1" between Russia and Estonia in 2007.[18] Cyberattacks can directly impact "real" infrastructure: "As computer networks collapse, factories and chemical plants explode, satellites spin out of control and the financial and power grids fail."[19]

In June 2010, for example, a computer worm called "Stuxnet" was discovered in Iran.[20] At first inspection, it appeared to be a routine bit of malware. Closer analysis, however, revealed that Stuxnet was carefully designed to disrupt the sort of systems that help control equipment at

16. *See infra* Part II.

17. *See Cyberwar: War in the Fifth Domain*, ECONOMIST, July 3, 2010, at 32, *available at* http://www.economist.com/node/16478792?story_id=16478792&CFID=158391401&CFTOKEN=34182131.

18. *Id.*

19. *The Threat from the Internet: Cyberwar*, ECONOMIST, July 3, 2010, at 50, *available at* http://www.economist.com/node/16481504?story_id=16481504&CFID=158391401&CFTOKEN=34182131.

20. Kim Zetter, *Clues Suggest Stuxnet Virus Was Built for Subtle Nuclear Sabotage*, WIRED THREAT LEVEL (Nov. 15, 2010, 4:00 PM), http://www.wired.com/threatlevel/2010/11/stuxnet-clues.

nuclear power plants.[21] Stuxnet's subtlety and sophistication suggested to most experts that it was engineered not by rogue hackers, but rather by an entity with the resources of a nation-state, and that it was specifically targeted to damage Iran's nuclear capabilities.[22] It almost certainly was a cyberattack launched by Israel or the United States.[23]

Recent evidence suggests that Stuxnet successfully curtailed Iran's production of refined uranium.[24] The Stuxnet attack appears to have bled into "real" space: the Iranian scientist chiefly responsible for eradicating Stuxnet from Iran's nuclear plants was killed on November 29, 2010, by assassins on motorbikes who stuck a bomb to his car.[25]

While Stuxnet is an example of a probable cyberattack by the United States and its allies, many experts believe that the United States is among the most vulnerable nations to a cyberattack. Every aspect of the U.S. economy and infrastructure depends on digital interconnections. Leading cybersecurity writer Richard Clarke suggests that "cyber war places this country [the United States] at greater jeopardy than it does any other nation."[26] Indeed, many experts believe that, even now,

> [c]omputer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States . . . .[27]

---

21. *Id.*

22. *Id.*; *see also* NICOLAS FALLIERE ET AL., W32.STUXNET DOSSIER (Symantec Security Response, Version 1.4, 2011), *available at* http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

23. *See* Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED THREAT LEVEL (July 11, 2011, 7:00 AM), http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (noting that "[s]uspicions of course were growing that Israel and the U.S. were behind Stuxnet and had used the malware as a devious alternative to bombing Iran's nuclear plant").

24. *The Stuxnet Worm: Yet to Turn*, ECONOMIST, Dec. 18, 2010, at 39, *available at* http://www.economist.com/node/17730556?story_id=17730556&CFID=158391401&CFTOKEN=34182131. It should be noted, however, that many cybercrimes are perpetrated by local Western individuals or low-level syndicates that disguise their attacks to appear as though they originate in "likely suspect" countries. *See* MCAFEE, INC., MCAFEE VIRTUAL CRIMINOLOGY REPORT: CYBERCRIME VERSUS CYBERLAW 12 (2009).

25. *The Stuxnet Worm: Yet to Turn*, *supra* note 24.

26. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT xiii (2010).

27. Shane Harris, *China's Cyber-Militia*, NAT'L J., May 31, 2008, at 32, *available at* http://nationaljournal.com/njmagazine/cs_20080531_6948.php; *see also* Ben Worthen, *Wide Cyber Attack is*

The Senate Committee on Commerce, Science, and Transportation recently reported that "[d]uring 2008, there were 54,640 identified [cyber]attacks against the Department of Defense; in 2009, there were 71,661 incidents reported; and through June 30 of 2010, there were 60,026 incidents reported."[28] Most analysts now agree that cyberwar is inevitable.[29]

Cyberspace also provides a home base for organized crime and terrorism. The distribution of malware designed to harvest personal and corporate information now is largely run by syndicates, many based in Russia, Nigeria, China, Brazil, or other organized crime havens, that control networks of tens of millions of infected computers called "botnets."[30] Cybercrime may cost the U.S. economy $1 trillion annually,[31] and cybercriminals frequently launder money through "virtual" worlds, such as Second Life.[32] Moreover, "there is a growing swell of opinion that [terrorist] hackers will eventually be bold enough and powerful enough to launch attacks that will damage and destroy critical national infrastructure."[33] In short, cybercrime, cyberterrorism, and cyberwar are synergistically blending into a massive perfect storm over the nation's information infrastructure.

B. Major Cybersecurity Proposals: 2009–2012

One of the most vexing policy issues raised by cybersecurity is that most critical physical cyber assets, such as routers, cables, servers, and interconnected machines and devices, are private property.[34] As the Senate Committee on Commerce, Science, and Transportation recently noted,

---

Linked to China, WALL ST. J., Mar. 30, 2009, at A18, *available at* http://online.wsj.com/article/SB123834671171466791.html.

28. S. REP. NO. 111-384, at 2 (2010).

29. PETER SOMMER & IAN BROWN, REDUCING SYSTEMIC CYBERSECURITY RISK 81 (2011), *available at* http://www.oecd.org/dataoecd/57/44/46889922.pdf ("[I]n nearly all future wars as well as the skirmishes that precede them policymakers must expect the use of cyberweaponry as a disrupter or force multiplier, deployed in conjunction with more conventional kinetic weaponry.").

30. *See Cyberwar: War in the Fifth Domain*, *supra* note 17.

31. CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE 2 (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

32. MCAFEE, INC., *supra* note 24, at 5.

33. *Id.* at 7.

34. *See, e.g.*, SOMMER & BROWN, *supra* note 29, at 6 (noting that "[l]arge sections of the Critical National Infrastructure of most OECD countries are in [sic] not under direct government control but in private ownership. Governments tend to respond by referring to Public Private Partnerships but this relationship is under-explored and full of tensions. The ultimate duty of a private company is to

> The private sector owns a large percentage of the nation's critical infrastructure, including electricity generation and transmission, water and sewer treatment facilities, and financial markets and clearinghouses. The computers that run these systems are often interconnected and subject to the same potential attacks as other networks. Experts suggest that cyber attacks against critical infrastructure potentially could physically destroy infrastructure, depriving large populations of essential goods and services for extended periods of time and threatening lives.[35]

Likewise, most intangible cyber assets—including data and cultural products—are either covered by private intellectual property rights and trade secrets or are in the public domain. Moreover, the very term "*cyber*security," with that curious prefix "cyber," highlights a basic question first raised at the dawn of the Internet age: who "owns" the Internet? The questions about presidential power explored in this Article, then, ask whether "cyberspace" is a sort of "space" over which the President can exert executive authority. The answers Congress has been exploring reflect a decidedly cyber-minimalist and executive power-maximalist approach: in a "cyber emergency," the President would possess the legal power to shut down—or at least significantly limit—public access to the Internet.[36]

The following subparts describe the major comprehensive cybersecurity proposals that Congress has considered over the past three years. It is instructive to explore each of these proposals in depth in order to survey the policy landscape and to examine how policymakers' views have changed—in form if not in substance—in response to concerns raised by civil society groups.

1. The Cybersecurity Acts of 2009 and 2010

The Cybersecurity Act of 2009 was introduced by Senators Rockefeller and Snowe on April 1, 2009.[37] Much of the bill was concerned with establishing technical standards and funding training, research, and

---

provide returns for its shareholders whereas a Government's concern is with overall public security and safety.").

35. S. REP. NO. 111-384, at 2 (2010).

36. Whether it is technologically possible to "shut down the Internet" is a different question.

37. S. 773, 111th Cong. (as introduced, Apr. 1, 2009); S. REP. NO. 111-384, at 5.

development in the field of cybersecurity. These provisions were relatively uncontroversial.[38]

More controversially, the 2009 bill would have delegated to the President various responsibilities relating to cybersecurity.[39] Under this proposed authority as set forth in the 2009 version of the bill, the President

> [m]ay declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network [and m]ay order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security.[40]

There were no time limitations, congressional or judicial review procedures, reporting requirements, or other substantive or procedural requirements attached to these provisions.

The bill was referred to the Committee on Commerce, Science, and Transportation, which held two hearings and reported out a revised bill, the "Cybersecurity Act of 2010," on March 24, 2010.[41] In the revised bill, the President's authority under the "cyber emergency" provisions was significantly muted.[42] The President would promulgate, after public notice and comment, a set of cyber emergency response plans.[43] The President would retain the authority to "declare a cybersecurity emergency," which would trigger implementation of the emergency response plans.[44] Within forty-eight hours after declaring a cybersecurity emergency, the President would be required to report to Congress, with supplemental reports every thirty days until the emergency declaration was removed.[45] The bill claimed that "[t]his section does not authorize, and shall not be construed to authorize, an expansion of existing Presidential authorities."[46]

---

38. S. 773 §§ 3–17 (as introduced, Apr. 1, 2009).
39. *Id.* § 18.
40. *Id.* § 18(2), (6).
41. S. 773, 111th Cong. (as reported by S. Comm. on Commerce, Sci., & Transp., Mar. 24, 2010); S. REP. NO. 111-384, at 5.
42. S. 773 § 201 (as reported by S. Comm. on Commerce, Sci., & Transp., Mar. 24, 2010).
43. *Id.* § 201(a)(1).
44. *Id.* § 201(b)(2).
45. *Id.* § 201(b)(3).
46. *Id.* § 201(c).

2. Protecting Cyberspace as a National Asset Act of 2010

The proposed Protecting Cyberspace as a National Asset Act of 2010 ("PCNA") was introduced by Senators Lieberman, Collins, and Carper on June 10, 2010.[47] Like the bill introduced by Senators Rockefeller and Snowe, the PCNA would have established an Office of Cyberspace Policy, with a director appointed by the President, and included provisions for enhancing communication, training, and emergency readiness regarding cybersecurity risks.[48] Also like the 2009 bill, the PCNA included exceptionally broad definitions of "cyberspace" and "information infrastructure." "Cyberspace" was defined as "the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[49] "Information infrastructure" was defined as "the underlying framework that information systems and assets rely on to process, transmit, receive, or store information electronically, including programmable electronic devices and communications networks and any associated hardware, software, or data."[50] And, like the 2009 bill, the PCNA would have authorized the President to declare a "national cyber emergency," which would trigger an Internet shutdown.[51]

Indeed, the enhancement of presidential authority in cyberspace was one of the primary goals of the PCNA. As a report on the bill prepared by the Senate Committee on Homeland Security and Governmental Affairs stated,

> The Committee understands that Section 706 [of the Telecommunications Act of 1934] gives the President the authority to take over wire communications in the United States and, if the President so chooses, shut a network down. But it is not clear that the President could order a lesser action, such as the blocking of a particular malicious signature or directing a company outside of the communications sector, such as an electricity generation facility, to

47. S. 3480, 111th Cong. (as reported by S. Comm. on Homeland Sec. & Governmental Affairs, Dec. 15, 2010); S. REP. NO. 111-368, at 15.

48. S. 3480 §§ 101–107.

49. *Id.* § 3(3).

50. *Id.* § 3(8).

51. *Id.* § 249.

> take action to protect its cyber networks. It is this gap that S. 3480 is meant to fill.[52]

The definitional procedural safeguards surrounding such a declaration, however, were enhanced in the PCNA—or at least they appeared enhanced upon a cursory reading.[53]

Under the PCNA, a "national cyber emergency" could be declared "if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure."[54] Although "cyber risk" was undefined, "risk" was defined as "the potential for an unwanted outcome resulting from an incident, as determined by the likelihood of the occurrence of the incident and the associated consequences, including potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident."[55] An "incident" included any occurrence that "actually or imminently jeopardizes" the security of or information within information infrastructure, as well as any occurrence that "constitutes a violation of security policies, security procedures, or acceptable use policies applicable to information infrastructure."[56]

In his or her declaration of a cyber emergency, the President would have been required to identify "covered critical infrastructure" implicated in the emergency.[57] The declaration would trigger an obligation for "owners and operators of [the] covered critical infrastructure" to implement a response plan.[58] The PCNA defined "critical infrastructure" with reference to the definition provided in the Patriot Act:

> [S]ystems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national

52. S. REP. NO. 111-368, at 10.

53. The committee report casts this in a positive, but ultimately ominous, light: "It would allow the President to take such action quickly, without any debate over what authorities the government actually has or the need to resort to the drastic measure of taking over an entire communications network." *Id.*

54. S. 3480 § 249(a)(1).

55. *Id.* § 3(19).

56. *Id.* § 3(7); *see id.* § 3551(b)(3).

57. *Id.* § 249(a)(2).

58. *Id.* § 249(a)(3)(A).

> economic security, national public health or safety, or any combination of those matters.[59]

The terms "owners" and "operators" were undefined. Response plans would have been required to comply with regulations to be issued by the Director of the Office of Cyberspace Policy ("DCP").[60] The bill stated that a determination that an asset is "critical infrastructure" may be appealed to the Secretary of Homeland Security, but that the Secretary's determination is not subject to judicial review.[61]

In addition to triggering the implementation of emergency response plans, the President's declaration of a cyber emergency would have empowered the DCP to enact additional "emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure."[62] Any such measures would need to reflect "the least disruptive means feasible to the operations of the covered critical infrastructure."[63] Emergency measures would expire after thirty days unless extended by the President, at the Director's recommendation, for successive thirty-day periods.[64] The owner or operator of the affected infrastructure would need to "immediately comply" with any emergency measures adopted by the DCP, unless and until the owner or operator could demonstrate to the Director that an alternative measure is feasible.[65]

The amended version of the bill included some specific limitations on the Executive's authority if an emergency is declared.[66] Some of these limitations seem ambiguous, if not self-contradictory. For example, the government could not "restrict or prohibit communications carried by, or over, covered critical infrastructure and not specifically directed to or from the covered critical infrastructure unless . . . no other emergency measure or action will preserve" the infrastructure's operation and mitigate disruption.[67] In other words, the government could prohibit such communications if necessary to limit disruption. In addition, the

59. *Id.* § 3(2).
60. *Id.* § 248.
61. *Id.* § 254(c).
62. *Id.* § 249(a)(3)(B).
63. *Id.* § 249(a)(3)(C).
64. *Id.* § 249(b).
65. *Id.* § 249(c).
66. *Id.* § 249(a)(6).
67. *Id.* § 249(a)(6)(A).

government could prohibit any communications "specifically directed to or from the covered critical infrastructure."[68]

Like the proposed Cybersecurity Act of 2009, then, the PCNA would have delegated to the President broad authority to shut down cyberspace. Although the Committee on Homeland Security and Governmental Affairs favorably reported the PCNA to the Senate, it was never scheduled for a floor vote and therefore expired.[69]

3. The Cybersecurity and Internet Freedom Act of 2011

In February 2011 Senators Lieberman, Collins, and Carper introduced a new bill that incorporated portions of the PCNA with some significant revisions and additions.[70]

The first portion of the bill, titled the "Internet Freedom Act," included a number of provisions designed to assuage the fears of cyber civil libertarians over prior cybersecurity bills.[71] The Internet Freedom Act included a congressional finding that "computer systems of executive branch agencies of the Federal Government and Congress are probed or attacked an average of 1,800,000,000 times per month" and that "cyber attacks can produce $8,000,000,000 in annual losses to the national economy."[72] Nevertheless, it noted that "the Internet has developed into a robust network within the United States, with thousands of providers, making it technically impossible to shut down the Internet."[73] It further stated that "the actions of the Government must not encroach on rights guaranteed by the First Amendment" and that "neither the President . . . nor any other officer or employee of the Federal Government should have the authority to shut down the Internet."[74] Finally, section 2(c) made clear that "neither the President . . . nor any other officer or employee of the

68. *See id.*

69. *See Bill Summary & Status, 111th Congress (2009–2010), S. 3480*, THOMAS, http://Thomas.loc.gov/cgi-bin/bdquery/z?d111:SN03480:@@@L&summ2=m&# (last visited Mar. 17, 2012).

70. Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

71. *Id.* § 2.

72. *Id.* § 2(b)(7)–(8).

73. *Id.* § 2(b)(4).

74. *Id.* § 2(b)(5), (10). In a statement introducing the bill, Senator Lieberman said, "We want to clear the air once and for all. As someone said recently, the term 'kill switch' has become the 'death panels' of the cybersecurity debate. There is no so-called 'kill switch' in our legislation because the very notion is antithetical to our goal of providing precise and targeted authorities to the President. Furthermore, it is impossible to turn off the Internet in this country." Press Release, Sen. Joseph Lieberman, Lieberman, Collins, Carper Introduce Bill to Address Serious Cyber Security Threats (Feb. 18, 2011), *available at* http://lieberman.senate.gov/index.cfm/news-events/news/2011/2/lieberman-collins-carper-introduce-bill-to-address-serious-cyber-security-threats.

United States government shall have the authority to shut down the Internet."[75]

Before examining the bill's substantive emergency provisions, it is useful to pause and reflect on the Orwellian quality of the "Internet Freedom Act." The bill's reassuring statement that the government must not encroach on the First Amendment is merely an obvious truism, which depends entirely on the meaning of "encroach." More oddly, the bill stated that it is impossible to "shut down" the Internet, before noting that nothing in the bill authorizes the President to do so.[76] Thus, the "Internet Freedom Act" would have assured the public that the President lacks congressional authorization to do the impossible. While it might be useful to know that Congress has not authorized the President to perform miracles, this seems to leave available any measure that is humanly possible. And so the "Internet Freedom Act," at best, recited the truisms that executive authority is bound by the First Amendment and the laws of physics.

The portions of the bill that specifically outline the President's authority in the event of a cyber emergency were only slightly less open-ended than the findings and restrictions in the "Internet Freedom Act." Section 249 on "National Cyber Emergencies" adopted the basic framework of the PCNA: it would require private owners of critical information infrastructure to implement emergency response plans in accordance with regulations to be issued by a new executive branch agency, the Office of Cyberspace Policy ("OCP").[77]

As in the PCNA, the 2011 bill recited several limitations on this broad regulatory authority, each of which, on careful examination, were illusory. First, the government could not "restrict or prohibit communications carried by, or over, covered critical infrastructure" unless such communications are "specifically directed to or from the covered critical infrastructure" or the OCP Director "determines that no other emergency measure or action" will effectively respond to the emergency.[78] The bill included no guidelines for the Director's "determination" under this subsection, nor were there any provisions for public notice and comment or judicial review.[79] Moreover, the "specifically directed to or from" carve out is potentially enormous if the infrastructure at issue comprises part of

75. S. 413 § 2(c). In an apparent response to backlash over the Senate committee report that accompanied the PCNA, this limitation extends also to section 706 of the Telecommunications Act of 1934. *Id.*

76. *Id.* § 2(b)(4), 2(b)(10), 2(c).

77. *Id.* §§ 101(a), 248(b)(2)(c), 249(a)(3)(A).

78. *Id.* § 249(a)(6)(A).

79. *See generally id.* § 249.

the Internet backbone. For example, because of how packet switching works, a malware attack against SCADA systems connected to the Internet likely would involve "communications" carried by and specifically directed to broad swathes of Internet backbone.[80]

The second limitation in the bill was that the government cannot "control covered critical infrastructure."[81] There was no definition of the term "control" and no further indication of what this limitation implies. Moreover, the bill would have required "owners and operators of covered critical infrastructure" to "immediately" implement their response plans upon the President's emergency declaration.[82] The bill further would have authorized the OCP Director to implement alternative emergency measures if the President declares a cyber emergency.[83] The Director would retain continuing discretion to review an owner or operator's emergency response plans and to require alternative measures.[84] There was no provision for public notice and comment or judicial review of the Director's determinations.[85] In other words, a private owner or operator's emergency plans could be set aside in the Director's discretion.

With this broad discretionary authority, the Executive obviously could exert significant control over covered infrastructure during an emergency.[86] It is true that the authority given in section 249 would not include the physical occupation of infrastructure facilities by police or military forces, and perhaps that is all the "no control" limitation covers. Even here, however, failure to comply could result in an uncapped civil penalty.[87] Failure to comply with a court order to pay a civil penalty, of course, could ultimately result in forfeiture of assets and/or a sanction for contempt of court. At best, therefore, the "control" limitation was hopelessly ambiguous.

The final set of limitations related to the authority to compel disclosure of information and conduct surveillance.[88] The first stated that the government may not "compel the disclosure of information unless specifically authorized by law."[89] The second clarified that the bill

80. *See, e.g.*, CLARKE & KNAKE, *supra* note 26.
81. S. 413 § 249(a)(6)(B).
82. *Id.* § 249(a)(3)(A).
83. *Id.* § 249(c)(1).
84. *Id.* § 249(c)(2).
85. *See generally id.* § 249.
86. *See id.* § 249(a)(3)(A).
87. *Id.* § 250(c)(1).
88. *Id.* § 249(a)(6)(C)–(D).
89. *Id.* § 249(a)(6)(C).

provided no surveillance or wiretap authority outside that which already exists under current law, including the Foreign Intelligence Surveillance Act of 1978 (FISA).[90] This surveillance and wiretap limitation seems chimerical in light of the broad authorities that already exist under FISA.[91] The information disclosure limitation was toothless because emergency security measures certainly would have included information reporting and auditing requirements authorized by the same law that includes this exception.[92] Section 250 of the bill, for example, would have required all owners and operators of covered critical infrastructure to submit a "certificate of compliance" with required security measures, subject to the Director's audit of "all documentation submitted" in support of the certificate, including a "a physical or electronic inspection of relevant information infrastructure" covered by the certificate.[93] Once again, these provisions at best seem to preclude only a large scale military or police seizure of information infrastructure facilities and data.

Any entity that violates the reporting and compliance requirements would be subject to an unspecified civil penalty.[94] The bill providedlimitations of civil liability for claims relating to cyber emergencies if the covered entity has complied with its emergency response obligations.[95]

An area in which the bill did provide substantial limitations not in the PCNA related to the duration of a state of cyber emergency. A declaration of cyber emergency would be effective for up to thirty days and could be extended for up to three additional thirty-day periods.[96] Subsequently, the state of cyber emergency could be continued only upon a joint resolution of Congress.[97] The PCNA, in contrast, would have permitted successive extensions by the Executive without further congressional oversight.[98]

Another way in which the bill differed from the PCNA is in the procedure for designating what comprises "critical information infrastructure," thereby triggering compliance obligations. The Secretary of Homeland Security would have been tasked with creating a list of

90. *Id.* § 249(a)(6)(D).
91. *See* discussion *infra* Part III.D.
92. *See, e.g.*, S. 413 § 250(a) (reporting), 250(b) (audit).
93. *Id.* § 250(a)(1), 250(b)(2)(A)–(B).
94. *Id.* § 250(c)(1).
95. *Id.* § 250(d)(2).
96. *Id.* § 249(b)(2).
97. *Id.*
98. *See* S. 3480, 111th Cong. § 249(b) (as reported by S. Comm. on Homeland Sec. & Governmental Affairs, Dec. 15, 2010).

critical information infrastructure resources, based on a variety of factors, including the extent of disruption, harm to the economy, and potential for mass casualties if the resource is compromised.[99] An owner or operator could appeal a designation in federal court in accordance with the Administrative Procedure Act.[100] This was the only specific provision for judicial review of any action by the Executive in the bill. This section of the bill also provided a mechanism for owners or operators to request that a system or asset under their control be designated as critical information infrastructure.[101] A determination made under this procedure would be unreviewable, not subject to any judicial review or other appeal.[102] Coupled with the limitations on civil liability under section 250, this provision would have offered a strong incentive to owners and operators to list themselves voluntarily. It is likely, for example, that large Internet backbone providers would list themselves in order to take advantage of the section 250 limitations on liability, thereby exempting these determinations even from the limited judicial review under the APA for involuntary designations.

4. The Cybersecurity Act of 2012

On February 14, 2012, Senators Lieberman, Collins, and Carper introduced yet another comprehensive cybersecurity proposal to replace the PCNA and the Cybersecurity and Internet Freedom Act of 2011—the Cybersecurity Act of 2012.[103] This bill does not contain any explicit authorization for the Executive to declare a cyber emergency. Supporters of the bill suggest that any potential "kill switch" language has been removed.[104]

However, section 109 would establish a procedure for "emergency planning," whereby the Secretary of Homeland Security would be authorized to create "response and restoration plans" with respect to critical infrastructure.[105] Such plans would empower the Secretary to "clarify specific roles, responsibilities, and authorities of government and

99. S. 413 §§ 502(a)(2)(B), 248(a)(2).
100. *Id.* § 254(c).
101. *Id.* § 254(d)(1)(A).
102. *Id.* § 254(d)(2).
103. S. 2105, 112th Cong. (as introduced, Feb. 14, 2012).
104. 158 CONG. REC. S617 (daily ed. Feb. 14, 2012) (statement of Sen. Joseph Lieberman) ("One myth about this bill is that it contains a kill switch that would allow the President of the United States in an emergency to seize control of the Internet. There is nothing remotely like that in this bill.").
105. S. 2105 § 109.

private sector entities when responding to a major cyber incident."[106] This section cross-references section 105(b) of the bill, which would authorize the Secretary of Homeland Security to enact regulations governing the cybersecurity compliance of owners and operators of critical infrastructure.[107]

It appears, then, that the question of Executive authority over the Internet in the event of a cyber emergency would, if this bill were adopted, remain a live question for the regulatory process. It might even make the problem more intractable since the bill provides no substantive guidance or limitations for any resulting regulations. In colloquial terms, it punts. In his floor comments in support of the bill, Senator Lieberman noted that "[a]t one time we had considered language that would, in fact, have limited powers the President has under the Communications Act of 1934 to take over electronic communications in times of war."[108] This narrowly defined presidential emergency power, he said, "was so widely misunderstood or misrepresented that we dropped it rather than risk losing the chance to pass the rest of this urgently needed legislation."[109] Given this belief of the bill's sponsors, and the language of the prior bills, the prospect of an open-ended rulemaking under the auspices of the Department of Homeland Security seems less than sanguine.

The ongoing debate over cybersecurity bills in Congress, therefore, demonstrates that problem of emergency executive authority in cyberspace remains intractable. Part III seeks to place this debate into a broader context by exploring the scope of presidential power in times of national emergency and specifically in relation to public safety and the Internet.

III. PRESIDENTIAL POWER AND CYBER EMERGENCIES

This Part explores the current scope of executive power in the event of a cyber emergency. It first examines inherent presidential powers under Article II of the U.S. Constitution. It then considers the principles of

106. *Id.* § 109(a)(2).

107. *Id.* § 105. The regulatory process envisioned in this section is a collaborative public-private model. *Id.* § 105(a).

108. 158 CONG. REC. S617 (daily ed. Feb. 14, 2012) (statement of Sen. Joseph Lieberman); *see also* Senator Joeseph Lieberman, Introduction of Cybersecurity Act of 2012 (Feb. 14, 2012), *available at* http://www.hsgac.senate.gov/download/senator-liebermans-statement-on-introduction-of-the-cyber security-act-of-2012 ("At one time we had considered language that would have limited sweeping powers we believe the President already has under the 'Communications Act of 1934' to commandeer all electronic communications in times of war. It would have narrowly defined the President's authority, not given him unbridled power.").

109. 158 CONG. REC. S617 (daily ed. Feb. 14, 2012) (statement of Sen. Joseph Lieberman).

delegated powers and examines aspects of communications and cybersecurity policy over which Congress has already delegated some degree of power to the Executive. This analysis will move a significant way towards a conclusion about the President's authority to shut down the Internet during a cyber emergency. This Article will also consider some occasions in which Congress has sought to regulate cybersecurity directly, in order to discern the Supreme Court's attitude towards civil liberties in cyberspace. That consideration is the subject of the subsequent Part.

A. Inherent Presidential Powers

The President possesses broad powers in times of war and national emergency, though the extent of constitutional restraints on those powers remains hotly debated.[110] The exercise of such inherent powers obviously raises separation of powers concerns. Such concerns are heightened when the President's exercise of war powers impinges on private property and rights of privacy. Because efforts to secure the national information grid necessarily implicate property and privacy rights, any such action should be subject to careful constitutional scrutiny.

The seminal case is *Youngstown Sheet & Tube Co. v. Sawyer*.[111] In 1951, in the midst of a labor dispute, President Truman issued an executive order directing the Secretary of Commerce to take over most the steel mills in the United States.[112] The President argued that he possessed inherent power to order the seizure because steel production was vital to national security, particularly in light of the Korean War effort.[113]

The Court held that the seizure exceeded presidential power under the Constitution.[114] Writing for the majority, Justice Black stated that, even if the President possesses some powers as Commander in Chief of the Armed Forces, "we cannot with faithfulness to our constitutional system hold that [the President] has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping

110. *See, e.g.*, Mark E. Brandon, *War and the American Constitutional Order*, *in* THE CONSTITUTION IN WARTIME: BEYOND ALARMISM AND COMPLACENCY 11 (Mark Tushnet ed., 2005); Mark Tushnet, *Emergencies and the Idea of Constitutionalism*, *in* THE CONSTITUTION IN WARTIME: BEYOND ALARMISM AND COMPLACENCY 39 (Mark Tushnet ed., 2005).

111. 343 U.S. 579 (1952).

112. *Id.* at 583.

113. *Id.* at 583–84.

114. *Id.* at 586–89.

production. This is a job for the Nation's lawmakers, not for its military authorities."[115]

In an often quoted and wide ranging concurring opinion, Justice Jackson offered three categories of presidential power: (1) "maximum" legitimacy, when the President acts under express authorization from Congress; (2) a "zone of twilight," when the President "acts in absence of either a congressional grant or denial of authority"; and (3) the "lowest ebb," when the President "takes measures incompatible with the expressed or implied will of Congress."[116] According to Justice Jackson, presidential actions in the first category are entitled to judicial deference, unless the underlying statute is unconstitutional.[117] Actions in the third category "must be scrutinized with caution," and should be upheld only if the Constitution expressly delegates authority to the President.[118] As to the second category's "zone of twilight," Justice Jackson stated, "any actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law."[119]

The steel seizure order, Justice Jackson argued, was unjustified under each category.[120] President Truman admittedly acted without express congressional authority, and his actions were in fact inconsistent with several existing statutes, eliminating the first and second categories.[121] As to the third category, Justice Jackson wrote at length about the dangers of executive control over civilian industries and other liberties even during wartime. "[T]he Constitution did not contemplate," he stated, "that the title Commander in Chief of the Army and Navy will constitute him also Commander in Chief of the country, its industries and its inhabitants."[122] Nevertheless, Justice Jackson left open the possibility that the President might exercise such power under exigent circumstances:

> The present situation is not comparable to that of an imminent invasion or threatened attack. We do not face the issue of what might be the President's constitutional power to meet such catastrophic situations. Nor is it claimed that the current seizure is in the nature of a military command addressed by the President, as

115. *Id.* at 587.
116. *Id.* at 635–38 (Jackson, J., concurring).
117. *Id.* at 635–37.
118. *Id.* at 637–38.
119. *Id.* at 637.
120. *Id.* at 638–55.
121. *Id.* at 638–39.
122. *Id.* at 643–44 (emphasis removed).

> Commander-in-Chief, to a mobilized nation waging, or imminently threatened with, total war.[123]

Because the nation was not engaged in total war and Congress had specified procedures for property seizures under ordinary circumstances, the steel seizure order exceeded presidential power.[124]

Justice Jackson's framework in *Youngstown* has gained special importance in response to the Bush Administration's assertions of executive authority while prosecuting the War on Terror.[125] In recent years, the assertion of presidential power reached its constitutional apogee in the "Torture Opinion" drafted by the Department of Justice's Office of Legal Counsel.[126] That opinion infamously argued that "Congress may no more regulate the President's ability to detain and interrogate enemy combatants than it may regulate his ability to direct troop movements on the battlefield."[127] It set off a press and academic firestorm, although no one was prosecuted for any actions taken in accordance with its advice.[128]

This backlash was perhaps reflected in the Supreme Court's recent disposition of a case touching on inherent presidential powers, *Medellin v. Texas*.[129] A group of Mexican nationals had been convicted of crimes in state courts in the United States.[130] The International Court of Justice determined in *Case Concerning Avena and Other Mexican Nationals* that these defendants were entitled to have their cases reconsidered due to violations of the Vienna Convention, even though the defendants failed to raise Vienna Convention claims in the state courts.[131] The Supreme Court subsequently held in *Sanchez-Llamas v. Oregon*, a case involving different

123. *Id.* at 659.

124. *Id.* at 660.

125. *See* Dawn E. Johnsen, *Faithfully Executing the Laws: Internal Legal Constraints on Executive Power*, 54 UCLA L. REV. 1559 (2007) (detailing the assertion of executive power during President Bush's prosecution of the War on Terror); Edward T. Swaine, *The Political Economy of* Youngstown, 83 S. CAL. L. REV. 263, 266 (2010) (noting, with respect to the renewed judicial and political interest in Justice Jackson's framework, "[w]hat a difference a war makes—especially an unpopular one").

126. *See* Johnsen, *supra* note 125, at 1566–73.

127. Memorandum from Jay S. Bybee, Assistant Att'y Gen., Office of Legal Counsel, to Alberto R. Gonzales, Counsel to the President, Re: Standards of Conduct for Interrogation Under 18 U.S.C. §§ 2340–2340A 35 (Aug. 1, 2002), *available at* http://www.washingtonpost.com/wp-srv/politics/documents/cheney/torture_memo_aug2002.pdf; *see also* Memorandum from John C. Yoo, Deputy Assistant Att'y Gen., Office of Legal Counsel, to William J. Haynes II, Gen. Counsel, Dep't of Def., Re: Military Interrogation of Alien Unlawful Combatants Held Outside the United States 13 (Mar. 14, 2003), *available at* http://www.aclu.org/pdfs/safefree/yoo_army_torture_memo.pdf.

128. *See* Johnsen, *supra* note 125, at 1567–68.

129. 552 U.S. 491 (2008).

130. *Id.* at 497–98.

131. *Id.*

defendants from those invoved in *Avena*, that the Vienna Convention did not bar "application of state default rules."[132] President Bush then issued a Memorandum to the Attorney General stating that the state courts should give effect to the *Avena* ruling.[133] In other words, the President directed that the *Avena* defendants could raise their Vienna Convention arguments notwithstanding the Supreme Court's *Sanchez-Llamas* opinion. Defendant Medellin appealed when the Texas courts refused to grant his application for a writ of habeas corpus.[134]

Medellin argued that the President's Memorandum rendered the ICJ's *Avena* decision binding in U.S. courts regardless of whether the Vienna Convention itself preempted state law.[135] The Court rejected this argument.[136] Citing "first principles" of limitations on presidential power, the Court noted that "Justice Jackson's familiar tripartite scheme provides the accepted framework for evaluating executive action in this area."[137] The Court concluded that neither the relevant treaties themselves nor the President's inherent foreign affairs powers authorized him to override state law in this instance.[138] Although *Medellin* is not a cybersecurity or War on Terror case, it suggests that the Court is perhaps becoming more sensitive to the limits of presidential power.

B. Delegated Powers and the Nondelegation Doctrine

Justice Jackson's first category of maximum legitimacy assumes that Congress may authorize the President to take certain actions. But what if Congress cedes Article I legislative powers to the President? The U.S. Constitution states that "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States . . . ."[139] Congress may not delegate its legislative powers to other branches of government.[140] The

132. *Id.* at 498 (citing Sanchez–Llamas v. Oregon, 548 U.S. 331 (2006)).

133. *Id.*

134. *Id.*

135. *Id.* at 523. The Court rejected Medellin's primary argument that the Vienna Convention did preempt state law. *Id.* at 504–23.

136. *Id.* at 523–32.

137. *Id.* at 524.

138. *Id.* at 523–32. In a dissenting opinion joined by Justices Souter and Ginsburg, Justice Breyer argued that the Vienna Convention preempted state law under the Supremacy Clause. *Id.* at 538–64 (Breyer, J., dissenting). Justice Breyer also concluded that the President's authority to implement U.S. obligations under the ICJ's *Avena* decision fell into the "middle range" of Justice Jackson's rubric. *Id.* at 564. Because the President's decision involved difficult foreign affairs policy questions, he stated, it should have been upheld. *Id.* at 565–66.

139. U.S. CONST. art. I, § 1.

140. *See generally* Mistretta v. United States, 488 U.S. 361 (1989).

Supreme Court has noted that "[t]he nondelegation doctrine is rooted in the principle of separation of powers that underlies our tripartite system of Government."[141] Any congressional authorization or delegation to the Executive therefore must satisfy the "nondelegation" doctrine.

The touchstone for nondelegation analysis is the "intelligible principle" test articulated by Justice Taft in *Hampton & Co. v. United States*: "If Congress shall lay down by legislative act an intelligible principle to which the person or body authorized . . . is directed to conform, such legislative action is not a forbidden delegation of legislative power."[142] The "intelligible principle" standard is quite broad. The Supreme Court has observed that "in our increasingly complex society, replete with ever changing and more technical problems, Congress simply cannot do its job absent an ability to delegate power under broad general directives."[143]

In fact, the Supreme Court has invalidated only two statutes for want of an intelligible principle for the exercise of executive discretion.[144] Both of these were New Deal cases decided in 1935—what Cass R. Sunstein has called the nondelegation doctrine's "one good year."[145] In *Panama Refining Co. v. Ryan*,[146] the Court evaluated the "Petroleum Code," an executive order that allocated oil production quotas among the States. The executive order was issued pursuant to the National Industrial Recovery Act ("NIRA"), a New Deal statute that authorized the President to issue trade standards for various key aspects of the economy.[147] The NIRA was enacted in response to a "national emergency"—the Great Depression.[148]

The Court first surveyed a variety of early precedents in which some delegation of rule-making authority to the Executive was upheld.[149] The Court derived from these cases a principle that the delegating statute must include some standards to constrain executive discretion.[150] Concerning oil production quotas, the Court noted, the NIRA "has declared no policy, has

141. *Id.* at 371.

142. 276 U.S. 394, 409 (1928) (upholding congressional delegation of authority to the President to adjust import tariffs).

143. *Mistretta*, 488 U.S. at 372.

144. Whitman v. Am Trucking Ass'ns, 531 U.S. 457, 474 (2001) (noting that "[i]n the history of the Court we have found the requisite 'intelligible principle' lacking in only two statutes" (citing Panama Ref. Co. v. Ryan, 293 U.S. 388 (1935); A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495 (1935))).

145. Cass R. Sunstein, *Nondelegation Canons*, 67 U. CHI. L. REV. 315, 322 (2000).

146. 293 U.S. 388 (1935).

147. *Id.* at 405–06.

148. *Id.* at 416–17.

149. *Id.* at 422–30.

150. *Id.* at 429–30.

established no standard, has laid down no rule."[151] The Court therefore directed the lower court to issue a permanent injunction against enforcement of the Petroleum Code.[152]

In *A.L.A. Schechter Poultry Corp. v. United States*, issued in the same year as *Panama Refining*, the Court examined the constitutionality of the "Live Poultry Code," which was promulgated by President Roosevelt under NIRA.[153] The NIRA authorized the President to approve "codes of fair competition" upon application by a trade or industry group or upon his own initiative.[154] Before approving a code, the President was required to find that the proposed code imposed no inequitable membership requirements and was not designed to promote monopolies.[155] The "Live Poultry Code" included wage, hour, and age regulations for poultry industry employees, and proscribed various unfair trade practices.[156]

The Court invalidated NIRA's delegation of authority to the President because the Act itself supplied no standards or rules of conduct for the regulated industry.[157] According to the Court, under NIRA, "the discretion of the President in approving or prescribing codes, and thus enacting laws for the government of trade and industry throughout the country, is virtually unfettered."[158]

C. Nondelegation and the War on Terror

Hampton and *Schechter Poultry* were the last and only cases in which the Supreme Court invalidated a statute or rule under the nondelegation doctrine. Even in historical context, these cases caused a political uproar over the Supreme Court's supervision of—or interference with, depending on political viewpoint—the New Deal.[159] The New Deal subsequently proceeded unhindered by judicial application of nondelegation principles. And the doctrine has fared no better in recent years, particularly in connection with national security and foreign relations issues. For example, lower courts and the Supreme Court have recently addressed nondelegation doctrine principles in the post-September 11 antiterrorism

151. *Id.* at 430.
152. *Id*. at 433.
153. 295 U.S. 495, 520–21 (1935).
154. *Id.* at 521–22.
155. *Id.* at 522.
156. *Id.* at 523–24.
157. *Id.* at 541–42.
158. *Id.* at 542.
159. *See* Sunstein, *supra* note 145, at 317–21, 326–28.

context. The issue surfaced somewhat obliquely in one of the seminal War on Terror precedents, *Hamdi v. Rumsfeld*.[160] In *Hamdi*, the Court reviewed the detention of an American citizen, without recourse to habeas corpus or other judicial procedures, at military facilities at Guantanamo Bay, Virginia, and South Carolina.[161] The Court held that citizen-detainees who seek to challenge their status as enemy combatants must receive notice and an opportunity to be heard before a neutral decision-maker.[162] En route to this holding, the Court addressed as a threshold question "whether the Executive has the authority to detain citizens who qualify as 'enemy combatants.'"[163]

A plurality led by Justice O'Connor found it unnecessary to address whether the President possessed plenary authority for these detentions under Article II of the Constitution.[164] The plurality located an express delegation of authority in the Authorization for Use of Military Force ("AUMF") issued by Congress the week after the September 11 attacks.[165]

The AUMF authorized the President to "use all necessary and appropriate force" against "nations, organizations or persons" that the President determined "planned, authorized, committed, or aided" the September 11 attacks.[166] The plurality stated that detention of enemy combatants "for the duration of the particular conflict in which they were captured, is so fundamental and accepted an incident to war" that it fell squarely within the "necessary and appropriate force" authorized under the AUMF.[167] The AUMF's "necessary and appropriate force" language, the plurality noted, constituted "explicit congressional authorization" for the detention of enemy combatants.[168]

Justice Souter, joined by Justice Ginsburg, concurred in the result but disagreed with the plurality's reasoning concerning the AUMF.[169] Justice Souter believed the true threshold issue was whether the AUMF was an

160. 542 U.S. 507 (2004) (plurality opinion).

161. *Id.* at 510–11. Hamdi was captured in Afghanistan while allegedly working for the Taliban. *Id.* at 510.

162. *Id.* at 533.

163. *Id.* at 516.

164. *Id.* at 517–25. Justice O'Connor's opinion was joined by Chief Justice Rehnquist and Justices Kennedy and Breyer.

165. *Id.*

166. Authorization for Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001).

167. *Hamdi*, 542 U.S. at 518 (plurality opinion).

168. *Id.* at 517.

169. *Id.* at 539–54 (Souter, J., concurring in part, dissenting in part, and concurring in the judgment).

"act of Congress" under the Non-Detention Act.[170] The Non-Detention Act, Justice Souter noted, was adopted in the wake of the Japanese internment camps during World War II.[171] The purpose of the Non-Detention Act, according to Justice Souter, was to "preclude reliance on vague congressional authority . . . as authority for detention or imprisonment at the discretion of the Executive . . . ."[172] For Justice Souter, then, the AUMF lacked the clarity and specificity required by the Non-Detention Act.[173] Nevertheless, he joined in the Court's judgment that Hamdi should be afforded a hearing on whether he was an enemy combatant.[174]

Justices Scalia and Stevens dissented because they believed "the Executive's assertion of military exigency" is never "sufficient to permit detention without charge" absent invocation of the Constitution's Suspension Clause by Congress.[175] According to Justice Scalia,

> Many think it not only inevitable but entirely proper that liberty give way to security in times of national crisis—that, at the extremes of military exigency, *inter arma silent leges.* Whatever the general merits of the view that war silences law or modulates its voice, that view has no place in the interpretation and application of a Constitution designed precisely to confront war and, in a manner that accords with democratic principles, to accommodate it.[176]

Justice Thomas, in contrast, dissented because he believed that Hamdi's detention "falls squarely within the Federal Government's war powers."[177] In ordering Hamdi's detention, the President, Justice Thomas concluded, acted both within the scope of his inherent Article II powers as Commander in Chief, and pursuant to a proper delegation of authority by Congress under the AUMF.[178] In the domains of foreign policy and national security, Justice Thomas stated, "the fact that Congress has provided the President with broad authorities does not imply—and the

170. *Id.* at 542. Under the Non-Detention Act, "[n]o citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress." 18 U.S.C. § 4001(a) (2006).

171. *Hamdi*, 542 U.S. at 542–43 (Souter, J., concurring in part, dissenting in part, and concurring in the judgment).

172. *Id.* at 543–44.

173. *Id.* at 551.

174. *Id.* at 553.

175. *Id.* at 554 (Scalia, J., dissenting).

176. *Id.* at 579.

177. *Id.* (Thomas, J., dissenting).

178. *Id.* at 580–99.

Judicial Branch should not infer—that Congress intended to deprive him of particular powers not specifically enumerated."[179]

Hamdi, then, while not specifically a "nondelegation doctrine" case, is an important contemporary source concerning the fraught tensions between individual constitutional rights and the powers of Congress and the Executive in the War on Terror context.

Some lower courts have addressed more explicit nondelegation challenges to War on Terror activities. In *United States v. Hammoud*, the Fourth Circuit considered a challenge to defendant Hammoud's conviction of providing material support to a foreign terrorist organization.[180] Hammoud provided support to Hizballah, which had been designated as a foreign terrorist organization ("FTO") by the Secretary of State pursuant to the Antiterrorism and Effective Death Penalty Act of 1996.[181] Among a panoply of constitutional and procedural arguments, Hammoud argued that the Secretary of State's designation of Hizballah as an FTO violated the nondelegation doctrine.[182] The court quickly disposed of this argument because, among other things, an FTO designation is subject to judicial review if challenged by the designated organization.[183]

In *Owens v. Republic of Sudan*, the plaintiffs sued the Republic of Sudan for injuries sustained in the 1998 bombings of the U.S. embassies in Kenya and Tanzania.[184] The suit was brought under the state sponsor of terrorism exception to the Foreign Sovereign Immunities Act.[185] Under this exception, a foreign sovereign designated by the Secretary of State as a state sponsor of terrorism lost sovereign immunity for claims arising out of acts of terrorism supported by an official, agent, or employee of the state.[186] The defendant claimed that the statutory exception improperly delegated to the Executive broad authority to invoke the jurisdiction of U.S. courts over foreign states.[187]

The court noted that "[a] statute that delegates factfinding [sic] decisions to the President which rely on his foreign relations powers is less susceptible to attack on nondelegation grounds than one delegating a

179. *Id.* at 583.

180. 381 F.3d 316 (4th Cir. 2004) (en banc), *vacated*, 543 U.S. 1097 (2005), *reinstated on remand*, 405 F.3d 1034 (4th Cir. 2005) (en banc). The original conviction was vacated because of an issue concerning the application of mandatory sentencing guidelines. *See Hammoud*, 405 F.3d at 1034.

181. *Hammoud*, 381 F.3d at 325–27 (citing 18 U.S.C.A. § 2339B (West 2000 & Supp. 2004)).

182. *Id.* at 331.

183. *Id.*

184. 531 F.3d 884, 886 (D.C. Cir. 2008).

185. *Id.*

186. *Id.* at 887–88 (citing 28 U.S.C. § 1605(a)(7) (2006)).

187. *Id.* at 888.

power over which the President has less or no inherent Constitutional authority."[188] The state sponsor of terrorism exception, the court stated, merely delegates to the Executive a fact-finding function well within its authority and expertise—the determination whether a particular foreign state is, in fact, sponsoring terrorism.[189] Moreover, the statutory definitions of "terrorism" and "international terrorism" provided sufficiently detailed parameters for guiding this determination.[190] Therefore, the court rejected the nondelegation challenge.[191]

D. Nondelegation, Government Power, and FISA

The post-September 11 torture memos were not the only aspect of the War on Terror that provoked deep concerns about the scope of presidential power in times of emergency.[192] A second key problem, with direct links to cybersecurity, was the President's authority to conduct surveillance in the United States.

The Bush Administration pressed its post-September 11 surveillance agenda, in part, through the Foreign Intelligence Surveillance Act ("FISA") and amendments to FISA under the Patriot Act.[193] The ensuing legal challenges were not cast as nondelegation doctrine issues, but the constitutional questions raised relate to the Executive's authority to monitor and regulate conduct on the Internet, and therefore raise related constitutional concerns.

FISA governs electronic foreign intelligence surveillance by the federal government.[194] FISA states that "the President, through the Attorney General, may authorize electronic surveillance without a court order . . . for periods of up to one year."[195] Such surveillance must relate to "communications transmitted by means of communications used exclusively between or among foreign powers" or "technical intelligence . . . from property or premises under the open and exclusive control of a foreign power."[196] "Minimization procedures" must be adopted to ensure that no communications involving a U.S. person are intercepted.[197]

---

188. *Id.* at 891.
189. *Id.* at 892–93.
190. *Id.* at 893 (citing 22 U.S.C. § 2656f(d)(1)–(2) (2006)).
191. *Id.*
192. *See supra* notes 115–16 and accompanying text.
193. *See* 50 U.S.C. § 1802 (2006).
194. *Id.*
195. *Id.* § 1802(a)(1).
196. *Id.* § 1802(a)(1)(A).
197. *Id.* § 1802(a)(1)(C); *see also id.* § 1801(i) (defining "United States person").

FISA also empowers the President to authorize the Attorney General to apply for court orders to conduct surveillance of communications between a foreign power or agent of a foreign power and a U.S. citizen.[198] Such requests must be directed to a secret court comprised of sitting federal judges ("FISA court").[199] In support of an application for a surveillance order, the government must provide details of the proposed surveillance and certify that "a significant purpose of the surveillance is to obtain foreign intelligence information."[200] Denials of such applications are subject to review by a special three-judge review court ("Court of Review").[201]

The "significant purpose" requirement was tested in the first opinion of the Court of Review, which remains one of the court's few published opinions, *In re Sealed Case*.[202] As discussed in *Sealed Case*, the "significant purpose" language was part of the Patriot Act's post-September 11 amendments to FISA.[203] FISA had previously required that "'the purpose' of the surveillance [was] to obtain foreign intelligence information."[204] Courts and the Department of Justice interpreted this to mean that FISA's requirements were not satisfied if the "primary purpose" of a FISA order was to gather evidence of a crime.[205] This contributed to the infamous "wall" between the FBI and the intelligence agencies, one of the key government communications breakdowns that facilitated the September 11 attacks.[206]

After the Patriot Act amendments to FISA, an interpretive difference arose between the Attorney General and the FISA court. The Attorney General understood the amended FISA to permit free information sharing between governmental intelligence and criminal functions—to break down completely the pre-September 11 "wall."[207] The FISA court, in contrast, required minimization procedures for all surveillance orders that

198. *Id.* § 1802(b).
199. *Id.* § 1803(a)(1), (c).
200. *Id.* § 1804(a)(6)(B).
201. *Id.* § 1803(b).
202. 310 F.3d 717 (FISA Ct. Rev. 2002).
203. *Id.* at 728–29.
204. *Id.* at 723 (emphasis added).
205. *Id.* at 725–27.
206. This is dramatically illustrated in the 9/11 Commission Report by the email of a frustrated FBI agent who was attempting to get information on Osama bin Laden's activities and was denied access because of the criminal/intelligence "wall": "Whatever has happened to this—someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'" NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 271 (2004).
207. *In re Sealed Case*, 310 F.3d at 729–30.

essentially reinstated the pre-September 11 Justice Department "wall" policies.[208]

The Court of Review held that "the FISA court erred" by requiring these procedures.[209] The Patriot Act amendments to FISA, the Court of Review held, were adopted specifically to minimize such distinctions.[210] So long as the government "articulates a broader objective than criminal prosecution," the statutory test is satisfied.[211]

The Court of Review then addressed whether the amended FISA violates the Fourth Amendment.[212] The concern raised by the ACLU was that, absent the "wall" procedures, a FISA order could be used as a substitute for a warrant required by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[213] The most significant difference between a Title III warrant and FISA order requirements, the Court of Review noted, is the standard for probable cause.[214]

A Title III warrant requires a showing that "'there is probable cause for belief that an individual is committing, has committed, or is about to commit'" a crime.[215] FISA requires only a showing "that the target is a foreign power or an agent of a foreign power."[216] However, the Court of Review noted that for a U.S. person to be considered an "agent of a foreign power" under FISA, that person must be engaged in some criminal activity on behalf of a foreign power.[217] Therefore, the court concluded, "FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security."[218] Moreover, the court believed that the particularity, necessity, duration, and minimization provisions in FISA, though in some instances less rigorous than Title III's warrant requirements, satisfied the Fourth Amendment's basic reasonableness test.[219]

---

208. *Id.* at 730.
209. *Id.*
210. *Id.* at 732–36. The Court of Review concluded that "the Patriot Act amendment, by using the word 'significant,' eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses." *Id.* at 735.
211. *Id.*
212. *Id.* at 736–42.
213. *Id.* at 737.
214. *Id.* at 737–40.
215. *Id.* at 738 (quoting 18 U.S.C. § 2518(3)(a) (2000)).
216. *Id.* (citing 50 U.S.C. § 1805(a)(3)).
217. *Id.*
218. *Id.* at 739.
219. *Id.* at 739–42.

The post-Patriot Act FISA survived a second constitutional challenge before the Court of Review in 2008.[220] In *In re Directives*, the Court of Review examined a Patriot Act amendment to FISA that permitted that acquisition of foreign intelligence surveillance information concerning persons "'reasonably believed' to be located outside of the United States."[221] Pursuant to this provision, the government directed a communication service provider to assist with warrantless surveillance of some of its customers.[222] The service provider contested the validity of those directives.[223]

The Court of Review first found that the service provider had standing to challenge the directives.[224] The court noted that the service provider "faces an injury in the nature of the burden that it must shoulder to facilitate the government's surveillances of its customers . . . ."[225]

However, the court rejected the service provider's constitutional challenge under the Fourth Amendment's warrant clause.[226] The Court of Review held that there is a "foreign intelligence exception" to the Fourth Amendment's warrant requirement.[227] Although the Supreme Court has not expressly recognized this exception, the Court of Review reasoned, it is available under the Court's "special needs" category of exceptions, which include drug testing and other public safety contexts.[228]

Consistent with its decision in *In re Sealed Case*, the Court of Review further held that to satisfy the "foreign intelligence" exception to the warrant requirement, the government need not show that the "primary purpose" of the surveillance is to gather foreign intelligence information.[229] Instead, the Court of Review held, "the more appropriate consideration is the programmatic purpose of the surveillances and

220. In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

221. *Id.* at 1006–07 (quoting 50 U.S.C. § 1805(b)(a)). The provision at issue expired pursuant to a sunset provision on February 16, 2008, and was not renewed. *Id.* at 1006 n.1. The identity of the service provider that challenged the directives is redacted in the public version of the decision.

222. *Id.* at 1007.

223. *Id.* at 1008.

224. *Id.* at 1008–09.

225. *Id.* at 1008.

226. *Id.* at 1009–16. The court quickly disposed of the service provider's facial challenge because the statute had in fact been applied in the context of the specific directives issued to the service provider. *Id.* at 1009–10.

227. *Id.* at 1010–12.

228. *Id.* at 1010–11.

229. *Id.* at 1011.

whether—as in the special needs cases—that programmatic purpose involves some legitimate objective beyond ordinary crime control."[230]

The Court of Review then examined the relevant government interest against the Fourth Amendment right to freedom from unreasonable searches and seizures under a "totality of the circumstances" test.[231] The "interest in national security," the court stated, "is of the highest order of magnitude."[232] The court rejected the petitioner's argument that the directives at issue lacked the sorts of safeguards—particularly, minimization procedures, targeting procedures, and judicial review—deemed important in *In re Sealed Case*.[233] As applied, the court held, the directives included reasonable safeguards, although most of the details about those procedures were redacted from the published opinion.[234]

In short, the courts thus far have upheld extensive warrantless cyber-surveillance under the amended FISA procedures.

E. Nondelegation and NSA Security Letters

The Bush Administration's surveillance agenda did not stop with FISA procedures. One of the most controversial aspects of the response to the September 11 attacks was President Bush's secret authorization to the National Security Agency ("NSA") to intercept international electronic communications between persons in the United States, including U.S. citizens, and suspected terrorists.[235] This secret surveillance was conducted without any warrant, FISA order, or other judicial oversight.[236]

When the NSA wiretap program was uncovered, it prompted a public outcry.[237] A coalition of constitutional law scholars and government officials, for example, argued to Congress that the Administration's position contradicted FISA's provision for wartime domestic electronic surveillance for a limited fifteen-day period and that Congress did not implicitly authorize domestic surveillance through the AUMF.[238]

---

230. *Id.*
231. *Id.* at 1012.
232. *Id.*
233. *Id.* at 1013.
234. *Id.* at 1013–14.
235. *See* Letter from William E. Moschella, Assistant Att'y Gen., to Sen. Pat Roberts, Chairman, Senate Select Comm. on Intelligence et al. (Dec. 22, 2005), *available at* http://www.justice.gov/ag/readingroom/surveillance6.pdf.
236. *See id.*
237. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program .html.
238. Letter from Curtis A. Bradley, Richard & Marcy Horvitz Professor of Law, Duke Univ. et al. to Sen. Bill Frist, Majority Leader, U.S. Senate et al. (Jan. 9, 2006), *available at* http://epic.org/

In response to these objections, the President grounded his power to conduct surveillance in his inherent authority as Commander in Chief, under Article II of the Constitution, to obtain signals intelligence, as supplemented by Congress' September 18, 2001 AUMF.[239] The Bush Administration reasoned that "[c]ommunications intelligence targeted at the enemy is a fundamental incident of the use of military force."[240] The Administration argued that the FISA procedures were not required because FISA expressly exempts from its provisions electronic surveillance otherwise "authorized by statute" and that the AUMF satisfied this exception.[241] Finally, the Administration claimed that the "special needs" exception to the Fourth Amendment's warrant requirement includes "[f]oreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States . . . ."[242]

The Electronic Frontier Foundation filed a class action lawsuit alleging privacy violations and other claims against telecommunications providers that allegedly cooperated with the NSA wiretap program.[243] Evidence submitted during the litigation suggested that the government had established a mirror site at a major Internet routing hub, which was capable of siphoning and reviewing enormous volumes of Internet traffic.[244]

The case was dismissed on the pleadings in the Northern District of California by District Judge Vaughn Walker.[245] Judge Walker held that FISA's immunity provision for service providers barred the plaintiffs' claims.[246]

---

privacy/terrorism/fisa/dojreply.pdf.

239. Letter from William E. Moschella, *supra* note 235, at 2–3.

240. *Id.* at 3.

241. *Id.* at 3–4.

242. *Id.* at 4.

243. Amended Complaint for Damages, Declaratory and Injunctive Relief, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-VRW), *available at* http://www.eff.org/files/filenode/att/att_complaint_amended.pdf; *see also* Letter from Cindy A. Cohn, Elec. Frontier Found., to Rep. John D. Dingell, Chairman, House Comm. on Energy & Commerce et al. (Oct. 12, 2007), *available at* http://w2.eff.org/Privacy/Surveillance/FISA/committee_letter.pdf.

244. *See* Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-VRW), *available at* http://www.eff.org/files/filenode/att/Mark%20Klein%20Unredacted%20Decl-Including%20Exhibits .PDF.

245. *In re* Nat'l Sec. Agency Telecomms. Record Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2009), *aff'd*,2011 WL 6823154 (9th Cir. 2011).

246. *Id.* at 955.

FISA's immunity provision was adopted specifically in response to the lawsuits filed after the public disclosure of the NSA wiretap program.[247] As Judge Walker noted, the immunity provision "creates a retroactive immunity for past, completed acts committed by private parties acting in concert with governmental entities that allegedly violated constitutional rights."[248] In order for immunity to apply, the executive branch, through the Attorney General, must certify that the statutory conditions for immunity have been met.[249]

The court rejected the plaintiffs' argument that this amounted to a legislatively mandated factual finding in violation of separation of powers principles.[250] Instead, the court held, it was merely an amendment to the law while litigation was pending, which is well within Congress's remit.[251]

The court also rejected the plaintiffs' argument that the certification requirement violated the nondelgation doctrine.[252] Judge Walker wrestled with the lack of an explicit charge from Congress to the Attorney General concerning which defendants should benefit from immunity.[253] The lack of such an express charge vests a substantial amount of discretion in the executive branch.[254] However, although Judge Walker considered this a "close question," he held that the statute could be construed in a way that preserves its constitutionality.[255] The immunity provision's legislative history and the "national security" context of the NSA program suggested to Judge Walker that Congress expected the Attorney General to approve immunity in most if not all cases pending against telecommunications companies, and this on balance provided enough direction.[256]

Judge Walker also disagreed with the plaintiffs' argument that the Attorney General's decision to file an immunity certification is a "final agency action" that must comply with the Administrative Procedure Act.[257] The court held that FISA's immunity provision contains its own

247. *Id.* at 958–59 (citing S. REP. NO. 110-209 (2007)).
248. *Id.* at 959.
249. *Id.* at 956–58.
250. *Id.* at 959–64.
251. *Id.* at 963–64.
252. *Id.* at 964–71.
253. *Id.* at 970.
254. *See id.*
255. *Id.* at 970–71.
256. *Id.* The court also rejected constitutional challenges to the immunity provision based on due process and free speech principles. *Id.* at 971–74.
257. *Id.* at 974–76.

"substantial evidence" standard for judicial review, which displaces any separate APA review.[258]

On December 29, 2011, the Ninth Circuit affirmed Judge Walker's Order.[259] The court rejected a variety of constitutional challenges to the immunity provision, including an argument under the nondelegation doctrine.[260] According to the court, the fact that the Attorney General has discretion whether to invoke the immunity provision in itself does not deprive the legislation of an intelligible principle for executive action.[261] The statute contains an intellible principle governing the Attorney General's conduct, the court held, because it identifies specific categories under which the Attorney General is authorized to exercise such discretion.[262]

As with cases concerning the FISA procedures, then, litigation challenging the warrantless wiretap program under nondelegation and related constitutional principles thus far has failed.

IV. TOWARDS A POLICY MATRIX FOR EXECUTIVE AUTHORITY AND CYBERSECURITY

Our discussion of cybersecurity and executive power thus far seems to leave us with few meaningful checks over the President's power to shut down cyberspace. In fact, the lawmakers who are sponsoring the current cybersecurity legislation believe the President already has authority to "shut down" the Internet under the Telecommunications Act of 1934.[263] However, in an important cyber-safety context not directly related to terrorism—child pornography—the Supreme Court, or at least some of its Justices, has signaled more of a cyber-exceptionalist posture that is significantly more wary of governmental regulation. Indeed, policy choices concerning presidential power and cybersecurity may turn as much on how lawmakers and courts construe "cyberspace" as on how they construe the Constitution.

This Part examines recent conflicting cyber-maximalist and cyber-minimalist strains of cybersecurity policy. The subsequent Part then offers

258. *Id.* Finally, the court also rejected plaintiffs' claims that the Attorney General's certification was substantively inadequate under FISA's immunity provision. *Id.* at 975–76.

259. *In re* Nat'l Sec. Agency Telecomms. Records Litig., 2011 WL 6823154 (9th Cir. 2011).

260. *Id.* at *5–14.

261. *Id.* at *7.

262. *Id.*

263. S. REP. NO. 111-368, at 10 (2010).

a matrix of options for presidential power and cybersecurity that incorporates the intersection of the cyber and constitutional domains.

A. Cyber-Minimalism: Cybersecurity and The Telecommunications Act of 1934

Perhaps the broadest recent assertion of executive authority over cyberspace was made in the report on the PCNA prepared by the Senate Committee on Homeland Security and Governmental Affairs. As noted above, the committee report stated that "[s]ection 706 [of the Telecommunications Act of 1934] gives the President the authority to take over wire communications in the United States and, if the President so chooses, shut a network down."[264]

Section 706 of the Telecommunications Act of 1934 delegates authority to the President to take emergency measures in times of war or national emergency:

> Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States . . . .[265]

The President's authority to assume control of privately owned communications lines was first exercised during World War I pursuant to a joint resolution of Congress.[266] A North Dakota state telephone system challenged the President's assertion of total control of telephone networks under the joint resolution.[267] The precise issue in the case was whether the President could regulate purely intrastate telephone rates.[268] The case reached the Supreme Court, which held that the joint resolution authorized

---

264. *Id.*

265. 47 U.S.C. § 606(c) (2006).

266. H.R.J. Res. 309, 65th Cong. (1918). The joint resolution stated that "the President during the continuance of the present war is authorized and empowered, whenever he shall deem it necessary for the national security or defense, to supervise or to take possession and assume control of any telegraph, telephone, marine cable, or radio system or systems, or any part thereof . . . ." *Id.* It required "just compensation" to be paid to the owners of such facilities. *Id.*

267. Dakota Cent. Tel. Co. v. South Dakota, 250 U.S. 163 (1919).

268. *Id.* at 170.

"the President to take complete possession and control to enable the full operation of the lines embraced in the authority," including the power to fix intrastate billing rates.[269]

During World War II, shortly after Congress's Declaration of War against Japan, President Roosevelt invoked his authority under § 706 to establish a Defense Communications Board, subsequently renamed the "Board of War Communications."[270] The Board of War Communications was authorized to allocate radio frequencies and facilities for military use.[271] However, the executive order stipulated that "[n]o radio station or facility shall be taken over and operated in whole or in part or subjected to government supervision, control or closure unless such action is essential to national defense and security and the successful conduct of the war."[272] The Board of War Communications was disbanded after the conclusion of World War II.[273] Since then, executive orders have provided that various agencies, including the Federal Communications Commission, should adopt contingency plans for war and national emergencies.[274]

The Telecommunications Act of 1934 and these historical examples of presidential authority under, of course, relate to the pre-Internet age. Would Internet services and infrastructure fall within the definition of "stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States" over which the President can assert control under § 706?[275] Read literally, this definition would cover any device powered by electricity. In conjunction with the reference to suspension or emendation of "rules and regulations applicable" to such "stations or devices," however, it seems clear that this section is referring to broadcast facilities and equipment already regulated by the federal government.[276]

Indeed, a recent FCC report on emergency preparedness equivocates over the FCC's authority to regulate cybersecurity infrastructure.[277] It

269. *Id.* at 184.

270. Exec. Order No. 8964, 6 Fed. Reg. 6367 (Dec. 12, 1941), *as amended by* Exec. Order No. 9183, 7 Fed. Reg. 4509 (June 17, 1942).

271. *Id.* §§ 1–4.

272. *Id.* § 5.

273. Exec. Order No. 9831, 12 Fed. Reg. 1363 (Feb. 26, 1947).

274. *See*, *e.g.*, Exec. Order No. 11,092, 28 Fed. Reg. 1847 (Feb. 28, 1963); Exec. Order No. 11,490, 34 Fed. Reg. 17,567 (Oct. 30, 1969); Exec. Order No. 12,656, 53 Fed. Reg. 47,491 (Nov. 18, 1988).

275. 47 U.S.C. § 606(c) (2006).

276. *Id.*

277. *See* PUB. SAFETY & HOMELAND SEC. BUREAU, FCC PREPAREDNESS FOR MAJOR PUBLIC EMERGENCIES: CHAIRMAN'S 30 DAY REVIEW (2009), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf.

notes that the scope of the FCC's authority depends upon whether an IP-based service is classified as a "telecommunications service" or an "information service" under the Telecommunications Act of 1996.[278] If an IP-based service is an "information service," the report notes, "the extent of the FCC's authority to regulate information services . . . has not been defined clearly."[279]

In fact, the question whether the Internet is a "telecommunications service" or an "information service"—or something else altogether—is the subject of intense debate.[280] As Susan Crawford notes, traditional telecommunications law involved two broad categories: "(1) regulated telephony, radio, and broadcast (dependent on radio or wired communications, and subject to 'public trustee' or common carriage obligations); and (2) largely unregulated newspaper and cinema (the 'print' model, not dependent on radio or wired communications)."[281] Congress has delegated regulatory authority to the FCC over broadcasters, telecommunications providers, satellite and cable providers, and wireless carriers, which fall into the first category.[282] Communication providers in the second category are unregulated by the FCC. The Internet, as Crawford observes, "sweeps aside" these regulatory "silos"; it combines aspects of each category and then transcends categorization by facilitating new human interaction.[283]

In short, the question is not merely one of regulating certain kinds of physical facilities. It is about the fundamental governance of culture. The Senate Committee on Homeland Security and Government Affairs' conclusion that § 706 authorizes the President to shut down the Internet, then, represents a dramatic and unprecedented assertion of authority over Internet governance. It stakes out a firm minimalist stance in the ongoing debate between cyber-exceptionalists and cyber-minimalists. Not all sources of cyber policy in American law would agree, as the following discussion on child pornography demonstrates.

---

278. *Id.* at 26.

279. *Id.*

280. *See, e.g.*, Susan P. Crawford, *Shortness of Vision: Regulatory Ambition in the Digital Age*, 74 FORDHAM L. REV. 695 (2005); Susan P. Crawford, *The Internet and the Project of Communications Law*, 55 UCLA L. REV. 359 (2007); Kevin Werbach, *Off the Hook*, 95 CORNELL L. REV. 535 (2010).

281. Crawford, *The Internet and the Project of Communications Law*, *supra* note 280, at 366 (footnotes omitted).

282. *Id.*

283. *Id.* at 366–70.

B. Cyber-Maximalism (or Cyber-Middle-ism): Child Pornography

Child pornography is one of the most hotly contested areas of what could broadly be called "cybersecurity." Although the problem of child pornography itself is not the focus of this Article, which is concerned with national security issue, cases involving online child pornography statutes are instructive concerning the difficult constitutional issues arising from efforts to regulate the Internet.

In *Reno v. ACLU* the Supreme Court addressed an effort by Congress to control Internet child pornography: the Communications Decency Act of 1996 ("CDA").[284] The CDA prohibited the knowing transmission of obscene or indecent messages to children less than eighteen years of age.[285] Among other things, it banned the use of "any interactive computer service to display [obscene material] in a manner available to a person under 18 years of age," and made it a crime to "knowingly permit" the use of a telecommunications facility "with the intent that it be used for such" purposes.[286] The statute included a good faith defense, and created a safe harbor for providers of Internet service and websites that required certain forms of proof of age, such as a credit card.[287]

The law was challenged by different groups of plaintiffs that included civil liberties organizations and library and publishing trade groups.[288] The Supreme Court found the challenged portion of the law unconstitutional.[289]

Writing for the Court, Justice Stevens sounded a remarkably exceptionalist note concerning Internet regulation. The Court had previously upheld government regulation of obscene and indecent speech involving the sale of pornography to minors, a radio broadcast of "filthy words," and a zoning ordinance segregating adult movie theaters from residential neighborhoods.[290] In each of these areas, Justice Stevens noted, the media involved were intrusive into daily life, and there was a long history of government regulation.[291]

But, he said, "[t]hose factors are not present in cyberspace."[292] Indeed, "[n]either before nor after the enactment of the CDA have the vast

284. 521 U.S. 844 (1997).
285. *Id.* at 859–60.
286. *Id.* at 860 (quoting 47 U.S.C. § 223(d) (1994 & Supp. II)).
287. *Id.* at 860–61.
288. *Id.* at 861–62 & nn.27–28.
289. *Id.* at 882.
290. *Id.* at 865–79 (citing City of Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986); FCC v. Pacifica Found., 438 U.S. 726 (1978); Ginsberg v. New York, 390 U.S. 629 (1968)).
291. *Id.*
292. *Id.* at 868.

democratic forums of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry."[293] And, he stated, "the Internet is not as 'invasive' as radio or television."[294] The CDA was invalidated because, in the unique context of the Internet, its restrictions were unconstitutionally vague and overbroad.[295]

In an opinion concurring in part and dissenting in part from the majority opinion, Justice O'Connor wrote that the creation of "adult zones" on the Internet could pass constitutional muster if the technology develops to a point at which screening for age is possible. Her view of the geography of cyberspace was perhaps even more exceptionalist than Justice Stevens's. While it is relatively easy to create adult-only zones in real space, she noted, "[t]he electronic world is fundamentally different."[296] In "cyberspace," Justice O'Connor said, speakers can mask their identities, locations, ages, and other distinguishing features, in a way that is not possible in the real world.[297]

Justice O'Connor also observed that cyberspace is "malleable," meaning that it may one day be feasible to "construct [virtual] barriers" between adults and children.[298] Such a "transformation of cyberspace," she concluded, however, had not yet progressed to the point at which age-related zoning could occur without unconstitutionally impinging on the First Amendment rights of adults.[299] However, Justice O'Connor would have upheld the CDA to the extent it covered a "transmission" of indecent materials between one adult and one or more minors.[300]

Congress regrouped after *Reno v. ACLU* and enacted a more focused child pornography law, the Child Online Protection Act ("COPA"). COPA applied only to "communication for commercial purposes" on the World Wide Web that was comprised of "material that is harmful to minors."[301] COPA was immediately challenged by the ACLU and other civil liberties groups and media entities.[302] The statute was examined by the Supreme Court on two separate occasions and then tested through a bench trial, ultimately resulting in a permanent injunction against its enforcement.[303]

---

293. *Id.* at 868–69.
294. *Id.* at 869.
295. *Id.* at 875–86.
296. *Id.* at 889 (O'Connor, J., concurring in part and dissenting in part).
297. *Id.*
298. *Id.* at 890.
299. *Id.* at 890–91.
300. *Id.*
301. 47 U.S.C. § 231(a)(1) (2000).
302. *See* Ashcroft v. ACLU (*Ashcroft I*), 535 U.S. 564, 571 n.4 (2002) (plurality opinion).
303. *See Ashcroft I*, 535 U.S. at 566–86 (plurality opinion); Ashcroft v. ACLU (*Ashcroft II*), 542

In its first trip to the Court, the Justices examined COPA's use of "community standards" to determine what sort of content is "harmful to minors."[304] This test was based on the Court's prior obscenity standard set forth in *Miller v. California*.[305] The appellate court had concluded that *Miller*'s community standards test was inapplicable to Internet communications and the Web "because 'Web publishers are currently without the ability to control the geographic scope of the recipients of their communications.'"[306] The Court disagreed that this problem of geographic under determination rendered the statute unconstitutional.[307]

Writing for a plurality, Justice Thomas sidestepped the geographic question by noting that "community standards need not be defined by reference to a precise geographic area."[308] This is particularly the case, Justice Thomas stated, when an obscenity statute precisely identifies material that will apply to the prurient interest and lacks serious value.[309]

In a concurring opinion, Justice O'Connor agreed that a "community standards" test could potentially be applied in the online environment, so that COPA was not facially unconstitutional.[310] However, she noted that divergent local community standards could support an as-applied challenge in a particular case.[311]

In a separate concurrence, Justice Breyer interpreted "community standards" in COPA to refer to a national adult community, which in his view allowed the statute to pass constitutional muster.[312] But if COPA were interpreted to require geographically local standards, Justice Breyer

---

U.S. 656 (2004); ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2008), *cert. denied*, 129 S. Ct. 1032 (2009).

304. *Ashcroft I*, 535 U.S. at 570. COPA defined "material that is harmful to minors" as material that

> (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

Id. (quoting 47 U.S.C. § 231(e)(b)).

305. *Id.* (citing Miller v. California, 413 U.S. 15 (1973)).

306. *Id.* at 575 (quoting ACLU v. Reno, 217 F.3d 162, 180 (3d Cir. 2000)).

307. *Id.* at 585–86.

308. *Id.* at 576.

309. *Id.* at 580.

310. *Id.* at 586–87 (O'Connor, J., concurring).

311. *Id.* at 587–88.

312. *Id.* at 589–91 (Breyer, J., concurring).

stated, this would "provide the most puritan of communities with a heckler's Internet veto affecting the rest of the Nation," and therefore would render the statute unconstitutional.[313]

Justice Kennedy authored yet another concurrence, joined by Justices Souter and Ginsburg.[314] Justice Kennedy believed the appellate court should have resolved various thorny questions of statutory interpretation before determining that the Act was facially unconstitutional.[315] For example, Justice Kennedy noted that the hyperlinked context of Web content must bear on "the vexing question of what it means to evaluate Internet material 'as a whole.'"[316]

Justice Stevens dissented.[317] For him, "[i]n the context of the Internet . . . community standards become a sword, rather than a shield."[318] This is because, he stated, "[t]he Internet presents a unique forum for communication because information, once posted, is accessible everywhere on the network at once."[319] He concluded, "[i]f a prurient appeal is offensive in a puritan village, it may be a crime to post it on the World Wide Web."[320] In the physical world, communities can self-segregate based on considerations, such as what sort of speech is tolerable.[321] However, Justice Stevens stated, this is impossible "in cyberspace."[322] A "community that wishes to live without certain material," he concluded, "rids not only itself, but the entire Internet, of the offending speech."[323]

The Court's first tussle with COPA thus highlighted the Justices' differing perspectives on Internet exceptionalism. For Justice Thomas, the Internet was merely instrumental to activities in physical space; for Justice O'Connor, it was an extension of activities in physical space, which could potentially be partitioned like real space; and for Justice Stevens, it was something irreducibly new.[324]

---

313. *Id.* at 590.
314. *Id.* at 591–603 (Kennedy, J., concurring).
315. *Id.* at 592.
316. *Id.* at 600.
317. *Id.* at 602–12 (Stevens, J., dissenting).
318. *Id.* at 603.
319. *Id.* at 605.
320. *Id.* at 603.
321. *Id.* at 612 ("Those who abhor and those who tolerate sexually explicit speech can seek out like-minded people and settle in communities that share their views on what is acceptable for themselves and their children.").
322. *Id.*
323. *Id.*
324. *See supra* notes 308–11, 317–23.

After remand, the Third Circuit once again upheld the preliminary injunction against COPA's enforcement, and the Supreme Court once again granted certiorari.[325] In a relatively terse opinion written by Justice Kennedy, the majority agreed with the lower court that blocking and filtering software offered a less restrictive alternative to COPA's broad legal prohibitions, and therefore upheld the preliminary injunction.[326] In a concurring opinion, Justice Stevens supplemented his Internet exceptionalist theme with a self-regulation note.[327] "Encouraging deployment of user-based controls," he stated, "would serve Congress' interest in protecting minors from sexually explicit Internet materials as well or better than attempting to regulate the vast content of the World Wide Web at its source, and at far less significant cost to First Amendment values."[328]

Justice Scalia dissented because he believed COPA should not have been subjected to strict scrutiny.[329] Justice Breyer wrote a separate dissent, joined by Chief Justice Rehnquist and Justice O'Connor.[330] According to Justice Breyer, COPA regulated only a very specific and narrow kind of obscene speech as permitted under *Miller v. California*.[331] Moreover, he was persuaded that web site proprietors could comply with the statutory age screening requirements at minimal cost—in other words, that it had indeed become technologically and economically feasible to zone the Internet.[332] Finally, he was not persuaded that filtering and blocking software was reliable enough or widely enough available to serve as a surrogate for legal regulation.[333] Ultimately, then, Justice Breyer adopted the moderate cyber-exceptionalism exhibited by Justice O'Connor in *Reno v. ACLU*.[334]

V. THE MATRIX

Cyberspace is different—or is it? The Internet is essentially a collection of physical assets that can be commandeered during war or national

325. *See* Ashcroft v. ACLU (*Ashcroft II*), 542 U.S. 656 (2004).
326. *Id.* at 667–68.
327. *Id.* at 673–75 (Stevens, J., concurring).
328. *Id.* at 674.
329. *Id.* at 676 (Scalia, J., dissenting).
330. *Id.* at 676–91 (Breyer, J. dissenting).
331. *Id.* at 678–79.
332. *Id.* at 682.
333. *Id.* at 685. Moreover, Justice Breyer noted that private filtering and screening software was the *status quo* against which COPA was enacted, not a less restrictive legislative alternative. *Id.* at 684.
334. *See supra* notes 296–300 and accompanying text.

emergency like telephone ground lines—or is it? The nondelegation doctrine and related constitutional checks supply few substantive restraints on presidential authority in times of war or national emergency—or do they? As the preceding Parts illustrate, courts have provided inconsistent answers to these questions. There does not appear to be a unified perspective on what "cyberspace" represents, or what degree of control the Executive should be empowered to assert over it.

A. Building the Matrix

It might be helpful to align differing answers to these questions in a policy matrix, as follows:

Cyberspace	Minimalist	Maximalist
Constitution / Non delegation	Minimalist	Maximalist

Cyberspace	Minimalist	Maximalist
Constitution / Non delegation	Minimalist	Maximalist

Cyberspace	Minimalist	Maximalist
Constitution / Non delegation	Minimalist	Maximalist

Cyberspace	Minimalist	Maximalist
Constitution / Non delegation	Minimalist	Maximalist

"Cyberspace" in this matrix refers to whether the Internet is considered a truly new, emergent "space" that transcends its physical layers or whether the Internet is essentially reducible to the cables, switches, and so on, that enable networked communication. "Maximalist" means the former; "Minimalist," the latter. "Constitution / Nondelegation" refers to the limitations the U.S. Constitution places on the President to control the Internet. "Minimalist" means Congress is able to delegate broad authority to the Executive to regulate the Internet; "Maximalist" means the Constitution strongly restrains what the Executive can do in this medium.

The recent bills in Congress reflect a "minimalist" perspective both on the nature of cyberspace and on the constitutional restrictions on the Executive's authority to control cyberspace.[335] This is most tellingly revealed in the report on the PCNA prepared by the Senate Committee on Homeland Security and Governmental Affairs, which asserted presidential authority over the Internet under a 1934 statute that addresses telephone lines.[336]

Indeed, the cyber-minimalism of the current congressional proposals is reflected even in the popular title of the PCNA. It is odd and incongruous for a bill in the Congress to describe "cyberspace" as a "national asset" of the United States. This perspective seems tone deaf to the ongoing debates over Internet governance, and in particular to the claim that the United States has historically sought to exert undue control over this global network.[337] This perspective stands in contrast to other sources of legal authority in the United States, particularly the Supreme Court's opinions on Internet pornography, which recognize that cyberspace is, indeed, in some sense unique.

Existing congressional proposals also are "minimalist" concerning the constitutional restrictions on the Executive. Although the recent proposals include some checks that move somewhat away from a hard "minimalist" view of the limits of the nondelegation doctrine—or at least "punt" such hard choices to a rule-making process—the Executive's discretion over whether to declare an emergency and what measures to take under such a declaration remains broad.[338] Perhaps most significantly, there is no provision for judicial review of emergency declarations or of any required emergency measures.[339]

B. Entering the Matrix

From a cyber-civil libertarian perspective, it is tempting to argue for a "maximalist-maximalist" option. Much of the opposition to the "Internet kill switch" in the blogosphere—including the term "kill switch"—reflects an assumption that the Internet is *sui generis* and that executive power over it should be sharply constrained. But the maximalist-maximalist perspective seems to lack the hard headedness required in the face of the

335. *See supra* Part II.B.
336. *See supra* note 52.
337. *See, e.g.*, Jonathon W. Penney, *Privacy and the New Virtualism*, 10 YALE J. L. & TECH. 194, 196–98 (2008) (describing historical debate).
338. *See supra* Part II.B.3.
339. *See supra* notes 79 and 85 and accompanying text.

very real threats posed by cyberwar, cybercrime, and cyberterrorism. If the scenarios and statistics offered in the recent spate of books and reports on cybersecurity are even half-true, the prospects for disruption are frightening.[340] A better approach is to recognize both the unique nature of the Internet and the unique role of the Executive in the event of war, a terrorist attack, or a disaster with respect to physical assets—that is, a framework that is cyber-maximalist but that adopts a sliding scale between constitutional minimalism and maximalism depending on the nature and scope of executive authority being asserted.

A key aspect of cyber-maximalism is commitment to the Internet's uniqueness. The debate over "cyberutopianism" or "exceptionalism," of course, has a long (in Internet time) history.[341] The "non-exceptionalist" thesis has been ably defended by Jack Goldsmith and Tim Wu, among others, who correctly observe that the Internet is physically comprised of routers, cables, servers, and other hardware that reside in real space under the jurisdiction of real sovereign governments.[342] Similarly, Orin Kerr notes that cyberutopianism is rooted in the political (and psychedelic consciousness bending) counterculture of the 1960s and has, along with that counterculture, largely been demolished by reality.[343]

But if cyberutopianism is dead, a realist conception of the new, emergent properties of the cultural construction facilitated by those routers, cables, and servers remains very much alive.[344] As Dan Hunter and Greg Lastowka have observed in relation to law in "virtual worlds," such as the game "Second Life," "virtual worlds are jurisdictions separate from our own, with their own distinctive community norms, laws, and rights."[345]

---

340. *See supra* Part II.A.

341. *See* Penney, *supra* note 337; *see also* Orin S. Kerr, *Enforcing Law Online*, 74 U. CHI. L. REV. 745, 751–54 (2007).

342. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

343. Kerr, *supra* note 341, at 752–54.

344. *See, e.g.*, David W. Opderbeck, *Deconstructing Jefferson's Candle: Towards a Critical Realist Approach to Cultural Environmentalism and Information Policy*, 49 JURIMETRICS J. 203 (2009).

345. F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CAL. L. REV. 1, 73 (2004). Cyberspace in this regard is very roughly analogous to the relationship between the brain and the mind. For a description of this relationship, see WILLIAM HASKER, THE EMERGENT SELF (2011), and NANCEY MURPHY, BODIES AND SOULS, OR SPIRITED BODIES? (2006). Brains are collections of neural cells, other tissues, and chemicals that are entirely physical. "Mind" emerges from these physical layers and comprises something new, with the capacity to exercise downward causation that continually reconfigures the physical layer.

One approach with some promise is the "denationalized liberalism" advocated by Milton Mueller.[346] Mueller recognizes that information transcends the boundaries of nation-states.[347] A denationalized liberalism, he suggests, "holds a presumption in favor of networked, associative relations over hierarchical relations as a mode of transnational governance."[348] Internet governance, he argues, "should emerge primarily as a byproduct of many unilateral and bilateral decisions by its members to exchange or negotiate with other members (or to refuse to do so)."[349] Nevertheless, because "people are deeply situated within national laws and institutions regarding such basic matters as contracts, property, crime, education, and welfare," national law must continue to play an important role, albeit a role that is "contain[ed]" by international associative relations.[350]

Although some of Mueller's ideasmight be problematic, he is on the right track. "Cyberspace" in some sense transcends the physical cables and switches that make the Internet possible. The Internet, therefore, is not merely a "national asset" of any state, and the security of "cyberspace" is an international concern that should be subject to international oversight. U.S. policymakers should take the lead in promoting the construction of a multilateral cybersecurity apparatus. The recognition that cybersecurity ultimately is an international Internet governance issue supplies an important interface with a modest account of constitutional limitations on the Executive's authority, particularly in relation to the nondelegation doctrine.

How can the nondelegation doctrine limit executive power over cyberspace? Given its generous interpretation, even in the heated context of the War on Terror, the nondelegation doctrine might seem dead in the water. Some commentators bemoan this fact and argue that it should be revitalized.[351] Paul Diller, for example, suggests that a revitalized nondelegation doctrine is particularly important in the wake of expanding

346. MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE (2010).

347. *Id.* at 269.

348. *Id.*

349. *Id.*

350. *Id.*

351. *See, e.g.*, Douglas H. Ginsburg & Steven Menashi, *Nondelegation and the Unitary Executive*, 12 U. PA. J. CONST. L. 251, 263–64 (2010) (arguing that "[w]hat is needed, in short, is a Court that recognizes that the nondelegation principle—although it is, like judicial review itself, a predominantly structural rather than a textual element—is no less a part of the judiciary's charge to uphold the Constitution").

executive power and the executive detention of terror suspects after September 11.[352]

Others, including Cass Sunstein, argue that "[r]eports of the death of the nondelegation doctrine have been greatly exaggerated."[353] Sunstein suggests that the nondelegation doctrine has been "relocated" into a series of smaller rules that he calls "nondelegation canons."[354] These rules restrict in various ways the ability of administrative agencies to make certain kinds of decisions without express congressional authorization.[355] He views these canons as an important democratic check on administrative agency action.[356]

As Sunstein acknowledges, a cornerstone of administrative law jurisprudence—the Chevron doctrine—is a pro-delegation rule, in that it permits agencies to invoke "reasonable" interpretations of their mandates if Congress has not directly decided the precise question under review.[357] However, he surveys a number of subsidiary canons that limit agency discretion even under Chevron.[358] The most significant, for purposes of this Article, are those related to sovereignty.[359] An agency cannot significantly compromise the sovereignty of a foreign nation, an Indian tribe, or the United States.[360] This related set of principles reflects the understanding that the Executive should not make sensitive judgments about national sovereignty and international relations without consulting Congress.[361]

While general principles of presidential authority recognize the Executive's unique role in conducting war and foreign affairs, this nondelegation "canon" relating to the sovereignty of foreign nations suggests that Congress should not—and perhaps cannot—authorize the

352. Paul Diller, *Habeas and (Non-)Delegation*, 77 U. CHI. L. REV. 585 (2010). Diller suggests that the Court's recent Suspension Clause jurisprudence weakens Congress's ability to craft flexible and robust alternatives to habeas corpus. *Id.* at 630–33. A better alternative, he argues, would have been for the Court to strike down the Combatant Status Review Tribunals established by the Bush Administration, which were ratified by Congress in the Detainee Treatment Act of 2005, as an improper delegation of authority to the President. *Id.* at 636–37. Diller notes that "Congress said almost nothing specific about how the CSRTs should function" and failed to define who was an "enemy combatant," and therefore did not provide even the requisite intelligible principle for the exercise of executive discretion. *Id.* at 637–41.

353. Sunstein, *supra* note 145, at 315.

354. *Id.* at 315–16.

355. *Id.* at 316.

356. *Id.* at 316–17.

357. *Id.* at 329.

358. *Id.* at 330–36.

359. *Id.* at 332–33.

360. *Id.*

361. *Id.*

President to control "cyberspace." Internet and other "cyber" communications emerge from global networks that implicate the sovereign interests of many states. As the World Summit on the Information Society's Declaration of Principles states "[p]olicy authority for Internet-related public policy issues is the sovereign right of States" (plural)—recognizing that no one State can control the Internet.[362]

The Declaration of Principles also assumes that international cooperation is vital because cyberspace truly is something sui generis, a new form of global culture. The Declaration notes, "[t]he Information Society is intrinsically global in nature and national efforts need to be supported by effective international and regional cooperation among governments, the private sector, civil society and other stakeholders . . . ."[363] Therefore, "building an inclusive Information Society requires new forms of solidarity, partnership and cooperation among governments and other stakeholders, i.e.[,] the private sector, civil society and international organizations."[364] The cybersecurity crisis further highlights the need for truly international and transnational Internet governance against broad assertions of authority by any one state, including the United States. The dual recognition in the Declaration—that States have sovereign rights because cyberspace implicates real space, but also that cyberspace requires unique international cooperation—should inform a sliding scale of constitutional "minimalism" or "maximalism" concerning U.S. cybersecurity policy.

When cyberattacks impact key physical infrastructure, the national sovereign requires the flexibility to act promptly and decisively. With this kind of limited impact, a sort of constitutional minimalism is appropriate. Constitutional minimalism in this context simply means that, with respect to physical assets located in American territory, the President can invoke emergency procedures when there is a significant threat to life, health, or the national economy. Even under such constitutional minimalism, emergency procedures must after a short contingency period become subject to direct congressional oversight and judicial review. However, broader deference should be afforded to the Executive's determinations. For example, a presidential order to shut down a nuclear power plant that

362. World Summit on the Information Society, Geneva 2003–Tunis 2005, *Declaration of Principles*, ¶ 49(a), U.N. Doc. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003), *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html.

363. *Id.* ¶ 60.

364. *Id.* ¶ 17.

has been infected by a Stuxnet-like malware attack would be subject to broad deference upon judicial review.

The scale should tip towards constitutional maximalism—in other words, stricter scrutiny—when emergency measures begin to impinge on the culture that emerges from cyber-infrastructure, particularly concerning core expressive concerns, such as the freedoms of speech, privacy, and association. For example, if the Executive claims that protecting the electricity grid from a cyberattack requires shutting down major Internet routing hubs, and thereby restricts the free flow of general email and Web communications, this measure should be subject to stricter scrutiny. Moreover, consistent with cyber-maximalism, any restrictions that will interfere with global Internet communications eventually should become subject to review by a multilateral international body. A policy space that incorporates these flexible safeguards will help protect the national security interests of the United States and other sovereign states with minimal interference over cyberspace's unique democratizing potential.

VI. CONCLUSION

Cyberspace is under constant attack. Because real space is increasingly connected to cyberspace, this means that facilities and institutions previously considered national resources—power grids, telephone communication systems, television networks, financial exchanges—are also cyber-resources. Under a system of constitutional democracy, as in the United States, the Executive must have some authority to take emergency actions required to protect such resources in the event of a natural disaster or an attack. This must include the authority to act in the face of a serious cyberattack.

But cyberspace is more than real space. Cyberspace's physical infrastructure facilitates the emergence of culture. This emergent property of cyberspace transcends national boundaries and bears enormous potential for democratization, as was vividly illustrated in Egypt's "Facebook Revolution." Yet, as Egypt's struggle also demonstrates—and as arguably has also been true of America's War on Terror—executive power over the Internet is a key arrow in the quiver of tyranny.

A balanced cybersecurity policy must account for all these dynamics. It must recognize the threat of cyberattack without losing—indeed, in light of—the uniqueness of cyber culture. It must require judicial scrutiny over emergency measures, on a sliding scale depending on the extent to which such measures are likely to impact cyber culture in addition to physical

assets. And it must tie in to an international framework, so that the promise of cyberspace can remain open to everyone.