MILITARY LAW REVIEW

Volume 206 **Winter 2010**

BUILDING A BETTER CYBERSECURITY ACT: EMPOWERING THE EXECUTIVE BRANCH AGAINST CYBERSECURITY EMERGENCIES

MAJOR JOHN S. FREDLAND*

I. "An Order of Magnitude Greater Economic Impact Than 9/11"[1]: Introduction

On July 19, 2008, a salvo of digital commands bombarded the official website of Georgian President Mikhail Saakashvili.[2] Bearing innocuous-sounding names like "flood http www.president.gov.ge/," "flood tcp www.president.gov.ge," and "flood icmp www.president.gov.ge," the commands rapidly rendered the presidential

* Judge Advocate, U.S. Air Force. Presently assigned as Staff Judge Advocate, National Air & Space Intelligence Center, Wright-Patterson Air Force Base, Ohio. LL.M., 2010, The Judge Advocate General's Legal Center and School, U.S. Army, Charlottesville, Virginia; J.D., 2000, Vanderbilt University Law School; B.A., 1997, Rice University. Previous assignments include Deputy Staff Judge Advocate, 92d Air Refueling Wing, Fairchild Air Force Base, Washington, 2007–2009; Appellate Defense Counsel, Appellate Defense Division, Air Force Legal Operations Agency, Bolling Air Force Base, D.C., 2005–2007; Area Defense Counsel, Air Force Legal Services Agency, Yokota Air Base, Japan, 2004–2005; Chief of Civil Law, 374th Airlift Wing, Yokota Air Base, Japan, 2003–2004; Chief of Legal Assistance, Operations Law and Claims, 12th Flying Training Wing, Randolph Air Force Base, Texas, 2000–2003. Member of the bars of Pennsylvania, the U.S. Court of Appeals for the Armed Forces, and the U.S. Supreme Court. This article was submitted in partial completion of the Master of Laws requirements of the 58th Judge Advocate Officer Graduate Course. The author would like to thank Major Robert Barnsby for his guidance, advice, and friendship throughout the writing process. He would also like to thank Major Christopher Ford and Major Benjamin Grimes for their insightful comments. Finally, the author would like to thank his parents, John W. Fredland and Kathleen Terleski, for their love and support.

[1] Nathan Gardels, *Mike McConnell: An American Cyber Expert on Cyberwar*, http://www.boozallen.com/consulting-services/services_article/42400037 (last visited Nov. 24, 2009).

[2] Posting of Steven Adair to Shadowserver Foundation, http://www.shadowserver.org /wiki/pmwiki.php/Calendar/2008720 (July 19, 2008, 21:57 EST) (on file with author).

website inoperable.[3] A cyberattack[4] had compromised Georgia's information infrastructure.[5]

Fortunately for Tbilisi, it had allies in cyberspace. An on-line cyberwatchdog group identified a U.S.-based server[6]—most likely infected by malicious code as a precursor to the distributed-denial-of-service attack[7]—as the seemingly unwitting command and control host for the cyberattackers' offensive.[8] Apparently eager to do their part for Georgia's national security, the private owner of the pirated server blocked the cyberattackers' access, ending the attack.[9]

The July 2008 cyberattack, occurring at a time of high tension between Tbilisi and Moscow,[10] proved to be mere prelude. On August 7,

---

[3] *Id.*

[4] This article includes derivatives of the root word "cyber," such as "cyberattack," "cyberinfrastructure," and "cybersecurity." "Cyber," with roots in author William Gibson's coinage of the term "cyberspace" in the 1984 novel *Neuromancer*, is an adjective that means "relating to computers or computer networks." Consequently, a cyberattack would be an attack carried out against a computer or computer network; cyberinfrastructure would be a country's computer network systems. Definition of "Cyber," MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com/dictiomary/cyber (last visited Jan. 12, 2010); Lieutenant Commander Matthew Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 2 n.4 (2009); David Wallis, *After Cyberoverkill Comes Cyberburnout*, N.Y. TIMES, Aug. 4, 1996, *available at* http://www.nytimes.com/1996/08/04/style/after-cyberoverkill-comes-cyberburnout.html.

[5] Posting of Steven Adair to SHADOWSERVER FOUNDATION, *supra* note 2 (on file with author).

[6] *Id.*

[7] Cyberattackers typically launch distributed-denial-of-service attacks from zombies, malicious code that entrenches itself inside a computer system and remains dormant until the attacker triggers it to action. Sklerov, *supra* note 4, at 15–16 nn.78, 85. *See infra* notes 50–54 and accompanying text (providing further discussion of denial-of-service attacks and distributed-denial-of-service attacks).

[8] Posting of Steven Adair to Shadowserver Foundation, *supra* note 2 (on file with author). Similarly, Project Grey Goose, a voluntary collaboration of cybersleuths, traced the July 2009 cyberattacks against the United States and South Korea, see *infra* notes 13–15 and accompanying text, to a Miami, Florida-based server belonging to a company called Digital Latin America, likewise without a criminal meeting of the minds between the cyberattackers and the private entity owning the hardware. *See* JEFFREY CARR, INSIDE CYBER WARFARE 78 (2010).

[9] Posting of Steven Adair to SHADOWSERVER FOUNDATION, *supra* note 2 (July 20, 2008, 13:36 EST) (on file with author).

[10] *Georgia Row Spirals as Rice Lands*, BBC NEWS, July 9, 2008, http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/7498340.stm (discussing tensions between Georgia and Russia that led to the South Ossetia War in August 2008).

heavy fighting erupted in and around the town of Tskhinvali in South Ossetia—the beginning of a five-day war between Georgia and Russia.[11] Almost simultaneously with the outbreak of kinetic combat, Georgian commercial and governmental websites experienced a wave of distributed-denial-of-service attacks, more substantial than the ones in July, rendering most governmental websites inoperable within two days and dramatically limiting governmental communication over the Internet.[12]

Cyberattackers have not restricted their digital barrage to Georgia. The United States' information infrastructure likewise stands as a frequent target. On a single day in 2008, the Pentagon experienced six million attacks from would-be cyberintruders.[13] Over the Independence Day weekend in 2009, distributed-denial-of-service attacks, tactically similar to those that Georgia faced in 2008, targeted several significant American governmental and commercial websites: the White House, Department of Homeland Security, Secret Service, National Security Agency, Federal Trade Commission, Department of the Treasury, Department of Defense, Department of State, New York Stock Exchange, NASDAQ Stock Market, Amazon, and Yahoo.[14] The attacks ultimately shut down the Treasury Department and Federal Trade Commission websites.[15] When the same network of fifty thousand computers targeted and shut down eleven websites of the South Korean government a few days later, military and political observers blamed North Korea for the attacks.[16]

These incidents have spurred American cyberwatchers and national security professionals to voice concerns about the potential for greater disasters involving the country's information infrastructure. Admiral Mike McConnell, former Director of National Intelligence, told an

---

[11] INDEPENDENT INTERNATIONAL FACT-FINDING MISSION ON THE CONFLICT IN GEORGIA, 1 REPORT 5 (2009), *available at* http://www.ceiig.ch/IIFFMCG_Volume_I.pdf.

[12] Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 A.F. L. REV. 43, 46 (2009).

[13] Ardaud de Borchgrave, *Silent Cyberwar*, WASH. TIMES, Feb. 19, 2009, *available at* http://www.washingtontimes.com/news/2009/feb/19/silent-cyberwar/.

[14] *U.S. Eyes N. Korea for "Massive" Cyber Attacks*, MSNBC.COM, July 9, 2009, http://www.msnbc.msn.com/id/31789294/ns/technology_and_science-security; MCAFEE, VIRTUAL CRIMINOLOGY REPORT 2009, at 4–5 (2009), *available at* http://resources.mcafee.com/content/NAMcAfeeCriminologyReport (last visited Mar. 4, 2010).

[15] *U.S. Eyes N. Korea for "Massive" Cyber Attacks*, *supra* note 14; MCAFEE, *supra* note 14, at 4–5.

[16] MCAFEE, *supra* note 14, at 4–6.

interviewer in 2009 that "[i]f the 19 terrorists who attacked the World Trade Center in 2001 had cyber-attacked one large New York bank and been successful in destroying the bank's data and backup data, we would have had an order of magnitude greater economic impact than 9/11 had on the world."[17] Later that year, McConnell informed *60 Minutes* that he believed that the United States's adversaries had the ability to bring down a power grid through cyberattack and that the "United States is not prepared for such an attack."[18] A Federal Bureau of Investigation (FBI) senior official testified to the Senate Judiciary Committee in 2009 that the "FBI is aware of and investigating individuals who are affiliated with or sympathetic to al Qaeda who have recognized and discussed the vulnerabilities of the U.S. infrastructure to cyber-attack."[19]

While cyberattacks represent a relatively recent addition to the United States's national security panorama, the events of the past two years demonstrate that America's foes, state and non-state alike, have the ability and inclination to attempt such attacks, with potentially severe consequences to vital security interests. Whenever the United States has faced threats to national security, policymakers and observers invariably have scrutinized the ability of the Executive Branch, the arm of Government best oriented for vigorous action in times of crisis,[20] to respond to those threats.[21] Cyberthreats warrant similar inquiry. To distill the issue to a concrete example: What power does the Executive Branch

---

[17] Gardels, *supra* note 1.

[18] *60 Minutes: Former Chief of National Intelligence Says U.S. Unprepared for Cyber Attacks* (CBS television broadcast Nov. 8, 2009) (transcript available at http://www.cbsnews/stories/2009/11/06/60minutes/main5555565.shtml). *But see* Evgeny Morozov, *Cyber-Scare*, BOSTON REV., July–Aug. 2009, *available at* http://www.boston review.net/BR34.4/morozov.php (downplaying concerns about cyberattacks by characterizing reports of cybercalamnies as being "usually richer in vivid metaphor—with fears of 'digital Pearl Harbors' and 'cyber-Katrinas'—than in factual foundation").

[19] Siobhan Gorman, *FBI Suspects Terrorists are Exploring Cyber Attacks*, WALL ST. J., Nov. 19, 2009 (discussing testimony of Mr. Steven Chabinsky, Deputy Assistant Dir. of the FBI's Cyber Div.).

[20] *See, e.g.*, AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 185–86 (Trade Paperback ed. 2006) ("[T]he framers aimed to infuse the executive branch with 'energy,' enabling it to master an unpredictable world by acting speedily where necessary . . . .").

[21] *See, e.g.*, NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 36–45 (2004) (detailing national crisis management response to 9/11 attacks); *Another War President, After All*, ECONOMIST, Jan. 7, 2010, *available at* http://www.economist.com/displaystorycfm?story_id=15213339 (discussing heightened scrutiny of U.S. intelligence and transportation security programs after attempted terrorist attempt to detonate bomb on commercial plane on Christmas 2009).

have to repel or neutralize a cybersecurity emergency of the sort that Georgia faced in 2008?

The nature of cyberspace complicates the analysis. Private industry owns most of the Internet, including network connections between various components of the U.S. Government.[22] If the United States discovered that a cyberattacker had purloined privately owned cyberinfrastructure to launch an attack, as Georgia's attackers did in July 2008, would it have to rely on the goodwill and patriotism of a private entity to stop the attack, or could it exercise its prerogative regardless of the private party's concurrence?[23]

Moreover, any potential Executive Branch action stands to raise many legal issues. Would any limits restrict the Executive Branch's power? What if its response stood to impair the free expression of an administration critic? Would the Government have to compensate the private entity for pecuniary loss? America's national security law regime for cybersecurity must contemplate these contingencies.[24]

In April 2009, Senator John D. "Jay" Rockefeller attempted to strengthen the Executive Branch's ability to protect the United States' governmental and commercial information infrastructure by introducing Senate Bill 773, the Cybersecurity Act of 2009.[25] The bill proposed, as part of a series of measures aimed at responding to cyberthreats,[26] authorizing the President to "declare a cybersecurity emergency and

---

[22] *See infra* Part II.A.

[23] *See* Todd A. Brown, *Legal Propriety of Protecting Defense Industrial Base Information Infrastructure*, 64 A.F. L. REV. 211, 244 (2009) ("[C]an the government legally impede a private network that it does not own, even if for a just purpose—protecting its networks?").

[24] Additionally, the Internet spans globally, creating many issues of international cooperation and jurisdiction. Could the United States, for example, act unilaterally if the private entity that owned the Internet hardware had citizenship in another country? *See, e.g.*, Ian MacLeod, *Canadian Producers Wary of U.S. Bills to Thwart Cyber Attacks on Power Grid*, CANADA.COM, Nov. 22, 2009, http://www.canada.com/technology/Electricity+industry+wary+bills+thwart+cyber+attacks/2253212/story.html (discussing Canadian concerns with "[f]our cyber-security bills before Congress contain[ing] either weak or no provisions requiring U.S. authorities to consult Canada before taking action to confront an imminent cyber threat to the continental network").

[25] Cybersecurity Act of 2009, S. 773, 111th Cong. (2009); *see infra* Part IV.A (discussing the specifics of the proposed Cybersecutiry Act).

[26] The measures included a cybersecurity advisory panel, security standards for Federal critical infrastructure information systems and networks, and a national licensing program for cybersecurity professionals. S. 773, § 3, at 6–7.

order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network"[27] and to "order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security."[28] This language provoked significant public concern.[29] Five months later, reports indicated that Senator Rockefeller's staff had drafted a revised bill, replacing the controversial language of Section 18 with new language.[30]

Whether President Barack H. Obama or a successor President will have the opportunity to turn specific legislation authorizing executive action against a cyberthreat remains unknown. The 111th Congress left office without taking action on Senator Rockefeller's bill after its initial

---

[27] *Id.* § 18(2).
[28] *Id.* § 18(6).
[29] *See, e.g.*, Larry Seltzer, *What Will the Cybersecurity Act of 2009 Do to Your Job and Business?*, EWEEK.COM, Apr. 10, 2009, http://www.eweek.com/c/a/Security/What-Will-the-Cybersecurity-Act-of-2009-Do-To-Your-Job-and-Business-768836/. Seltzer expressed the concern that

> we won't know what [will qualify for federal control] until the president says. He can designate bank networks, perhaps critical common carriers, or whatever else he thinks is critical. Then, in the event of "cyber-attack," he can order those shut off or disconnected. I think Congress owes it to us to put a more solid definition in the bill so that it can be discussed in hearings, on the record, rather than letting the president decide unilaterally.

Id. See also Steve Aquino, *Should Obama Control The Internet?*, MOTHER JONES, Apr. 2, 2009, *available at* http://motherjones.com/politics/2009/04/should-obama-control-internet; Bob Chapman, *Controlling the Ability of People and Organizations to Access the Internet*, PPJ GAZETTE, Feb. 19, 2010, http://ppjg.wordpress.com/2010/02/19/controlling-the-ability-of-people-and-organizations-to-access-the-internet/ ("Sitting ominously in the Senate is the Rockefeller Bill S. 773 to take over the Internet in emergencies. As we all know, once taken over, we will never get it back the way it was before. This is what elitists have in mind for us.").
[30] Declan McCullagh, *Bill Would Give President Emergency Control of Internet*, CNET NEWS, Aug. 28, 2009, http://news.cnet.com/8301-13578_3-10320096-38.html. This new language provided that "in the event of an immediate threat to strategic national interests involving compromised Federal Government or United States critical infrastructure information system or network" the President could "declare a cybersecurity emergency." It further provided that "if [the President] finds it necessary for national defense and security, and in coordination with relevant industry sectors, [the President would] direct the national response to the cyber threat and the timely restoration of the affected critical infrastructure information system or network." *See infra* Part IV.B (discussing the reported changes).

introduction in the Senate's Committee on Commerce, Science, and Transportation.[31] Regardless of the pace, priorities, and preferences of the Legislative Branch, however, cyberthreats figure to haunt America's national security landscape throughout the foreseeable future. This backdrop renders it necessary to evaluate the Executive Branch's legal ability to respond to such threats, and to demand better legal tools if the current legal regime proves inadequate.

This article argues that the current state of the law gives the Executive Branch a poor framework for protecting governmental and commercial information infrastructure during cybersecurity emergencies. To provide background on the operational environment, Part II addresses the nature of the cybersecurity battlefield. It focuses on three aspects of the United States's governmental and commercial information infrastructure—the reliance on privately owned hardware, nature of cyberattacks, and ease of violating the sovereign prerogative of neutrality—creating a need for decisive Executive Branch action to preserve national security.

Part III examines relevant precedents, statutes, and practices to determine the Executive Branch's current legal position to respond to cyberattacks or preserve U.S. neutrality. This survey finds that a lack of directly applicable case law and other legal authority make legislative action necessary to empower the Executive. Part IV assesses the strengths and weaknesses of Senator Rockefeller's cybersecurity legislation. It concludes that the proposed Cybersecurity Act of 2009 represented an improvement over the current state of the law but suffered from significant shortcomings, specifically in oversight and compensation for aggrieved parties. Finally, Part V proposes a revised Cybersecurity Act, with safeguards similar to the Federal Intelligence Surveillance Act of 1978[32] and the War Powers Resolution.[33] Ultimately, the article concludes that the current security environment and uncertain state of legal authority render such a bold proposal necessary to address concerns about oversight and compensation, while still allowing the Executive Branch a definite legal basis for intervening in cybersecurity emergencies.

---

[31] *S.773—Cybersecurity Act of 2009*, OPEN CONGRESS, http://www.opencongress.org/bill/111-s773/actions_votes (last visited Mar. 4, 2010) (tracking progress of bill).

[32] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, §§ 103, 104(a)(7)(A)–(C), 92 Stat. 1783, 1788–89 (1978) (codified as amended at 50 U.S.C. §§ 1801–1863 (2006)).

[33] 50 U.S.C §§ 1541–1548 (2006).

II. The Cybersecurity Battlefield

A. "The Control System of Our Country"[34]: The Rise of Cyberspace

The multitude of interconnected computers, servers, routers, switches, and fiber optic cables known as cyberspace enjoys an all-pervasive position in modern life.[35] When President George W. Bush issued the United States's first *National Strategy to Secure Cyberspace* in 2003,[36] the document identified cyberspace as "the control system of our country," linking "agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping."[37] Massive portions of the economy, both nationally and worldwide, depend on cyberspace.[38]

In the beginning, cyberspace—and its most prevalent form, the Internet—stood as the sole domain of the U.S. Government. The Pentagon's Advanced Research Projects Agency created ARPAnet in 1969 to allow computer scientists and engineers working on military contracts to share computers and other resources, regardless of their physical locations.[39] By the mid-1980s, the system, now known as the "internet," had expanded minimally, still confined to a "cloistered world"

---

[34] THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 1 (2003) [hereinafter CYBERSPACE NAT'L STRATEGY].

[35] *Id.* (describing components of cyberspace). *See generally* Memorandum from the Sec'y of the Air Force & the Chief of Staff, U.S. Air Force, to all Airmen, subject: Air Force Cyberspace Mission Alignment (Aug. 20, 2009), *available at* https://newafpims.afnews.af.mil/shared/media/document/AFD-090821-046.pdf (noting that cyberspace "pervades every other domain and transcends national boundaries"); Sklerov, *supra* note 4, at 3–4 (discussing the importance of the Internet).

[36] CYBERSPACE NAT'L STRATEGY, *supra* note 34.

[37] *Id.* at 1.

[38] *See, e.g.*, ANDREW COLARIK, CYBER TERRORISM: POLITICAL AND ECONOMIC IMPLICATIONS, at viii–xi (2006) (observing that trillions of dollars of electronic banking and global stock trading are conducted over the Internet each year); TRADE PROMOTION COORDINATING COMMITTEE, 2008 NATIONAL EXPORT STRATEGY (2008) (discussing the "explosive growth of the Internet and e-commerce," including a projection that business-to-consumer e-commerce in the United States will grow from $175 billion in 2007 to $335 billion in 2012).

[39] P.W. SINGER, WIRED FOR WAR: THE ROBOTICS REVOLUTION AND CONFLICT IN THE 21ST CENTURY 52–53 (2009); Christopher Anderson, *Like a Flock of Birds: How the Internet Works Without Really Trying*, ECONOMIST, July 1, 1995, *available at* http://www.temple.edu/lawschool/dpost/accidentalsuperhighway.htm.

of military laboratories and universities.[40] Private sector network computing had experienced a relatively limited parallel development; local area networks for businesses and commercial "on-line" services had emerged but had not spread widely.[41]

Dramatic transformation, morphing cyberspace from a government undertaking into a private-sector enterprise, occurred in the late 1980s and early 1990s. By this time, the National Science Foundation (NSF) had assumed responsibility for funding and organizing the U.S. Government's network.[42] In 1988, the NSF, seeking to avoid the likelihood that separate private and public development channels would make cyberspace a piecemeal entity, allowed private organizations to join the network but restricted them from using it for commercial purposes.[43]

Over the next seven years, the U.S. Government eliminated all remaining curbs on commercial use.[44] In April 1995, the NSF finally discontinued its role as the Internet "backbone" and began to phase out the last direct federal subsidies for the network.[45] The Internet had transformed from a purely governmental enterprise to a private entity. Because of this shift, the U.S. Government now relies on countless private entities to sustain its own cyberinfrastructure; these private parties also serve as ports of entry for state and local governmental cyberinfrastructure and commercial cyberinfrastructure.[46]

---

[40] Anderson, *supra* note 39 (indicating that by "1987 the Internet had grown to include 28,000 host computers at hundreds of different universities and research labs"); *The Launch of NSFNET*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/nsf0050/internet/launch.htm (last visited Jan. 12, 2010) [hereinafter *The Launch of NSFNET*].

[41] Anderson, *supra* note 39.

[42] *Id.*

[43] *Id.*; *The Launch of NSFNET*, *supra* note 40 (quoting Steve Wolf, NSA Program Dir., as stating, "[I]t was obvious that if [commercial interests could not join the Internet] in a coordinated way, it would come in a haphazard way").

[44] Anderson, *supra* note 39.

[45] *Id.*; *An End and a Beginning*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/nsf0050/internet/anend.htm (last visited Jan. 12, 2010).

[46] *See, e.g.*, Brown, *supra* note 23, at 212 (noting private ownership of "the network connections between various components of the Air Force[], and even more broadly, the U.S. government[]"); MCAFEE, *supra* note 14, at 21 ("Creating further challenges, much of the communications, software and network infrastructure is owned and operated by the private sector.").

B. Denial-of-Service, Zombies, and Packet Sniffers: The Weapons of Cyberspace

The various private entities comprising the United States' governmental and commercial cyberinfrastructure stand vulnerable to many types of cyberattack—attacks that could, in turn, trigger the sort of national security emergency requiring the Executive Branch to compel a private entity to cease the operation of its Internet hardware. The July 2008 attack against Georgia's cyberinfrastructure, for example, involved a cyberattacker's apparently pirated use of a server owned by a U.S.-based private company as a launching point for the attacks.[47] To develop an effective legal structure for empowering the Executive Branch to respond to cyberemergencies, policymakers must first understand the nature of the threat. Students of cybersecurity have identified three main categories of cyberattacks: automated malicious software delivered over the Internet, denial-of-service (DOS) attacks, and unauthorized remote intrusions into computer systems by individuals.[48] All three may require a private entity to take action to halt a cybersecurity emergency.

Internet-delivered malicious software, or malware, generally affects computer systems through infected e-mails, engines designed to exploit vulnerabilities, or visits to infected websites.[49] Initially, malware fell into two broad classifications: viruses and worms.[50] Programmers and attackers have subsequently generated a diverse array of malicious code, including Trojan horses, rootkits, sniffers, exploits, bombs, and zombies.[51]

Denial-of-service attacks overwhelm targeted computer systems with information until the systems seize up and cannot function, preventing access by legitimate users.[52] Distributed-denial-of-service (DDOS) attacks, the sort of cyberattack that crippled Georgia's cyberinfrastructure, represent the most severe form of a DOS attack.[53] They involve launching DOS attacks simultaneously from numerous

---

[47] *See supra* notes 1–9 and accompanying text.
[48] *See* Sklerov, *supra* note 4, at 13–14 n.62 (expressing the opinion that cyberattacks can be divided into three main categories, but indicating that other authors have claimed two main categories or four main categories).
[49] *Id.* at 14.
[50] *Id.* at 14–15.
[51] *Id.* at 15–16.
[52] *Id.* at 16.
[53] *Id.*

computers; their sheer volume makes them difficult to defend.[54] Cyberattackers frequently set the stage for DDOS attacks by launching "zombies," a strain of malware that can entrench itself into computer systems until cyberattackers trigger it into action.[55] The resulting juggernaut of zombie-infected computers, harnessed into a coordinated DDOS attack, is known as a "botnet."[56]

The third type of cyberattack, a remote intrusion, involves penetration of a computer system by an unauthorized user.[57] Occurring at user access points, remote intrusions require an attacker to obtain user account names and passwords.[58] This happens through malware or by using social engineering, packet sniffers, and password cracking tools to acquire user account information.[59] Unauthorized access leaves an attacker in position to harm a system in a variety of ways, including "caus[ing] a cascading series of damages in the physical or electronic world."[60]

All three varieties of cyberattack may place private entities in the unsuspecting position of having their computer hardware facilitate a potential cyberattack. A malware worm, for example, may use an unwittingly infected server as a launching point for spreading from system to system, copying itself to any computer systems connected to the infected computer.[61] The July 2008 DDOS attack that shut down the website of the President of Georgia used a hijacked computer belonging to a private company in the United States.[62] Professor Jack Goldsmith has observed that the "United States has the most, or nearly the most, infected botnet computers [in the world] and is thus the country from which a good chunk of botnet attacks stem."[63] Having successfully accomplished a remote intrusion into a utility company's computer system, an attacker may use that base to access critical infrastructure. The legal regime governing the Executive Branch's response to such cyberemergencies should empower the Executive to take action to stop

---

[54] *Id.*
[55] *Id.* at 16 n.78.
[56] *Id.* at 16 n.85.
[57] *Id.* at 17.
[58] *Id.*
[59] *Id.*
[60] *Id.* (quoting COLARIK, *supra* note 38, at 84.) .
[61] *Id.* at 15.
[62] *See supra* notes 1–9 and accompanying text.
[63] Jack Goldsmith, *Can We Stop the Global Cyber Arms Race?*, WASH. POST, Feb. 1, 2010, at A17.

these private entities' hardware from damaging critical governmental or commercial information infrastructure, but still provide meaningful limitations on the Government's power.

C. "Such Assistance and Succor to One of the Belligerents"[64]: Cyberattacks and Neutrality

Cyberwatchers and national security professionals concerned about the operational implications of cyberspace have generally focused on a cyberattack's ability to impair critical governmental and commercial information infrastructure.[65] Emerging scholarship, however, contends that cyberattacks may also affect a state by unwittingly drawing it from a neutral position into a conflict between two other states.[66] Because international law imposes a dramatically different legal status on states that enter conflicts between other states as a belligerent, compared with states electing to remain neutral, the choice between belligerency and neutrality represents one of the most significant responsibilities for a sovereign's national security decision-making body. Because of this potential hazard of the operational realm of cyberspace, crafting a legal regime that both governs the Executive Branch's power over cyberspace and provides for vigorous action to preserve U.S. neutrality when a U.S.-based party's conduct potentially jeopardizes that neutrality is essential.

In his influential 1906 treatise on international law, the German jurist Lassa Oppenheim defined neutrality as "the attitude of impartiality towards belligerents adopted by third States and recognized by belligerents, such attitude creating rights and duties between the impartial States and the belligerents."[67] Specifically, Oppenheim, tracing the development of neutrality as part of international law from its inception in the sixteenth century,[68] regarded neutrality as incompatible with "such assistance and succor to one of the belligerents as is

---

[64] 2 LASSA OPPENHEIM, INTERNATIONAL LAW: A TREATISE: WAR AND NEUTRALITY 317 (1906).
[65] *See supra* notes 17–19 and accompanying text.
[66] *See* Kastenberg, *supra* note 12 (providing a full discussion of the application of the principles of neutrality to cyberspace).
[67] OPPENHEIM, *supra* note 64, at 316.
[68] *Id.* at 302. Oppenheim identified the roots of neutrality in Middle Ages treaties entered into "for the purpose of specially stipulating that the parties should be obliged not to assist in any way each other's enemies during time of war, and to prevent their subjects from doing the same." *Id.* at 316.

detrimental to the other, and further, such injuries to the one as benefit the other."[69] Moreover, he observed that international law obligated states to guard their neutrality through "active measures," with a requirement to "prevent belligerents from making use of their neutral territories and of their resources for military and naval purposes during the war."[70]

Oppenheim published his treatise a year before the 1907 Hague Convention V on "The Rights and Duties of Neutral Powers and Persons in Case of War on Land"[71] and Convention XIII on "The Rights and Duties of Neutral Powers in Naval War,"[72] the modern codification of neutrality law. Echoing Oppenheim's formulation of neutrality, Hague Convention V articulated a relatively straightforward relationship between belligerency and neutrality. Article 1 declared the territory of a neutral state to be "inviolable."[73] Articles 2–4 listed acts violating a state's neutrality; the list included routing men or materials, erecting communications devices, and recruiting forces on the territory of a neutral state.[74] Article 5, however, established the "price" of neutrality for a state seeking neutral status—the imperative to prevent any of the acts listed in Articles 2–4 from occurring on its territory.[75] This imposed a "policing burden" on states desiring neutrality.

> If a neutral is unable or unwilling to effectively enforce its right of inviolability, an aggrieved belligerent may act proportionately and as necessary to counter enemy forces' actions, including actions by enemy warships and military aircraft making unlawful use of neutral territory.

---

[69] *Id.* at 317.
[70] *Id*.
[71] Convention Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague Convention V].
[72] Convention Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415, 1 Bevans 723 [hereinafter Hague Convention XIII].
[73] Hague Convention V, *supra* note 71, art. 1.
[74] *Id.* arts. 2–4. The 1907 Hague Convention V does provide a limited telecommunications exception. Article 8 dictates that a "neutral power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus," provided that the neutral state allows all belligerents equal use of the communications facilities. *Id.* art. 8. Legal experts have questioned whether this exception applies to cyberspace and cyberattacks. *See* Kastenberg, *supra* note 12, at 56.
[75] Hague Convention V, *supra* note 71, art. 5.

> Today this right is tempered by the [United Nations] Charter in that an aggrieved belligerent must be a target of an armed attack, actual or threatened, from neutral waters to exercise this power.[76]

Of course, the architects of international law in the first decade of the twentieth century did not contemplate cyberspace or cyberattacks. More than a century after the Hague Conventions' enactment, their general conception of neutrality remains controlling law,[77] but international law does not explicitly address cyberattacks and cyberneutrality.[78] The development of the details of neutrality law has proven difficult to predict; one commentator observed that it "defies a straightforward, positivist, black-letter approach."[79] Nevertheless, commentators attempting to gauge the direction of neutrality law have applied the fundamental principles of the Hague Conventions to the cyberbattlefield and concluded that three aspects of recent cyberconflicts have threatened to compromise U.S. neutrality in international conflicts where the U.S. Government claimed an official position of neutrality.[80]

The 2008 cyberattack against Georgia exemplifies the first aspect: an attack routed across the Internet nodes of a neutral state.[81] Because approximately eighty percent of the Internet's traffic traverses the United States, America stands extremely vulnerable to having its neutrality compromised in this manner.[82] An August 2008 article by Evgeny Morozov, an Internet journalist residing in the United States, suggested an example of the second aspect: cyberattacks launched from a neutral state but uncontrolled by that neutral state.[83] The article demonstrated

---

[76] George K. Walker, *Information Warfare and Neutrality*, 33 VAND. J. TRANSNAT'L L. 1079, 1145 (2000).
[77] *See id.* at 1128 ("[N]eutrality, primarily as practiced in the nineteenth century, has been modified in the Charter era, but the general concept of neutrality remains.").
[78] Kastenberg, *supra* note 12, at 53.
[79] Walker, *supra* note 76, at 1109. The American jurist Philip Jessup asserted in 1936 that neutrality law has "undergone an almost constant process of revision in detail," driven by "compromise and experience." PHILIP C. JESSUP, NEUTRALITY: TODAY AND TOMORROW 16, 156 (1936).
[80] Kastenberg, *supra* note 12, at 53; Walker, *supra* note 76, at 1079.
[81] Kastenberg, *supra* note 12, at 53.
[82] *Id.* at 43.
[83] *Id.* at 53; *see also* Evgeny Morozov, *An Army of Ones and Zeroes—How I Became a Soldier in the Georgia-Russia Cyberwar*, SLATE, Aug. 14, 2008, http://www.slate.com/id/2197514; *see also* EVGENY MORZOV, http://evgenymorozov.com/blog/?p=416 (last visited Jan. 14, 2010).

that anyone with access to the Internet could have visited a website, downloaded software, and joined the DDOS attacks against Georgia in minutes.[84]

The third neutrality-threatening aspect of recent cyberconflicts happened during the August DDOS attacks against Georgia.[85] When the cyberattacks imperiled the Georgian Government's use of its own information infrastructure, two U.S.-based private companies, Tulip Systems and Google, allowed Georgia to use their hardware for governmental Internet services.[86] Neither company attempted to obtain the U.S. Government's consent for their actions.[87] The United States did not suffer any immediate consequences, but, as a commentator asserted, "the actions of the Georgian government and a well-intentioned, patriotic [in favor of Georgia] CEO could have imperiled U.S. cyber neutrality."[88]

Because of the severe consequences of entering an international conflict as a belligerent, the United States' national security decision-makers have few responsibilities more important than determining whether America adopts a stance of belligerency or neutrality in an international conflict. The neutrality-threatening aspects of cyberconflict threaten to undermine that prerogative. All three circumstances identified in this section may require the Executive Branch to take coercive action over a private entity to maintain America's neutrality in a foreign conflict—forcing the owner of the pirated server to shut down operations, stopping the individual from launching a cyberattack from U.S. soil, and halting the efforts of a sympathetic CEO to protect another country's cyberinfrastructure, if U.S. national security interests require it. Otherwise, the actions of private parties may subject the United States to physical attack. For this reason, the United States' legal regime on cybersecurity should contemplate and facilitate action in the interest of addressing an internal threat to U.S. neutrality.

---

[84] Kastenberg, *supra* note 12, at 53. In a January 2010 speech on "Internet freedom," Secretary of State Hillary Clinton spoke approvingly of the efforts of "hacktivists," who use digital tools to fight oppressive regimes. As Professor Jack Goldsmith noted, "[s]cores of individuals and groups in the United States design or employ computer payloads to attack government websites, computer systems and censoring tools in Iran and China." Goldsmith, *supra* note 63. The international law implications of the U.S. Government's encouragement of such efforts fall outside of the scope of this article.

[85] Kastenberg, *supra* note 12, at 60–61.

[86] *Id.*

[87] *Id.*

[88] *Id.* at 61.

III. "Zone of Twilight"[89]: The Current State of Executive Legal Authority

If the United States found itself in a similar position as Georgia in July 2008, with hijacked privately owned computer hardware enabling a cyberattack against critical governmental infrastructure or compromising an official position of neutrality, it would most likely seek the shutdown of that hardware. The U.S. Code, however, currently contains no statutes directly addressing Executive powers in a national security emergency over the private entities comprising cyberspace.[90] As a result, a President seeking to impose the coercive power of the U.S. Government under such circumstances would have to rely on some combination of the Constitution, case law, other statutes, and prior Executive Branch practice as legal authority for his actions. This article's first inquiry, then, seeks to determine the current state of Executive authority in this area.[91] It reveals a lack of directly applicable legal authority, strongly suggesting a need for congressional action.

Before considering the state of the law, it bears noting that American political philosophy does provide authority for an Executive to act notwithstanding the law in a time of national crisis. Thomas Jefferson articulated this principle in an 1810 letter to John B. Colvin.[92] In that letter, Jefferson, who had left the presidency in the previous year, indicated that "laws of necessity, of self-preservation, of saving our country when in danger, are of higher obligation" than the written law, under certain circumstances.[93]

---

[89] Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 637 (1952) (Jackson, J., concurring).

[90] One recent commentator asserted that his article on the Executive Branch and cyberneutrality would "[suggest] a rubric using existing laws for exerting executive authority," but did not cite any provisions of the U.S. Code concerning Executive Branch authority. Kastenberg, *supra* note 12, at 45. In February 2010, a federal judge in Virginia granted Microsoft's request for an order to deactivate hundreds of Internet addresses that the company had linked to a botnet. Nick Wingfield & Ben Worthen, *Microsoft Battles Cyber Criminals*, WALL ST. J., Feb. 26, 2010, *available at* http://online.wsj.com/article/SB10001424052748704240004575086523786147014.html. Because the court issued its order under seal, precluding analysis of its theory of injunctive relief, this article does not consider the ruling's implications for the Executive Branch's cybersecurity efforts. *Id.*

[91] *See generally* Henry P. Monaghan, *The Protective Power of the Presidency*, 93 COLUM. L. REV. 1, 138 (1993) (discussing theories and sources of Executive power).

[92] Letter from Thomas Jefferson, to John B. Colvin (Sep. 20, 1810), *available at* http://teachingamericanhistory.org/library/index.asp?document=1916.

[93] *Id.*

Jefferson postulated, however, that the Executive official would not be immune from consequences: "[T]he good officer is bound to draw it at his own peril, and throw himself on the justice of his country and the rectitude of his motives."[94] Such a situation, of course, would be extremely undesirable; extra-legal action by government officials should remain an option of last resort.[95] In that light, it is incumbent upon the Executive Branch to find pre-existing legal authority empowering it to act coercively or to request that Congress pass appropriate legislation to provide the necessary powers.

A. *Youngstown Sheet & Tube Co. v. Sawyer*: The Steel Seizure Case

The Supreme Court's majority opinion and concurrences in *Youngstown Sheet & Tube Co. v. Sawyer* (*Steel Seizure*)[96] represent the leading source of guidance on the Executive Branch's "emergency" power over the private sector[97] in the absence of congressional action authorizing the Executive to act. Employing a variety of constitutional theories and frequently stressing the ruling's narrowness, the opinions ultimately prove an inconclusive source of guidance on the state of Executive power in the event of a cyberattack. The various opinions provide material suggesting that the Executive would have some measure of coercive power over the private parties, but the extent of that power—as well as any constitutional limitations on it and the details of its implementation—remains uncertain. This suggests that legislation which expressly articulates Executive power and clarifies roles and responsibilities would be beneficial for ensuring the United States' ability to respond to cybersecurity challenges promptly, while satisfying the demands of the Constitution and republican government.

---

[94] *Id.*

[95] Whether any of the Presidents of the United States have, in fact, acted in accordance with Jefferson's "pragmatic concession to necessity" approach is unknown. One commentator has observed that "[s]ome version of the precept seems to lie behind Abraham Lincoln's suspension of provisions of the Constitution during the Civil War." Mark E. Brandon, *War and American Constitutional Order*, 56 VAND. L. REV. 1815 (2003).

[96] 343 U.S. 579 (1952).

[97] *See, e.g.*, Robert J. Reinstein, *The Limits of Executive Power*, 59 AM. UNIV. L. REV. 259, 259 (2009) (calling Justice Jackson's concurrence in *Youngstown* the "prevailing doctrine of presidential power").

1. "Indispensable"[98]*: Executive Order and Legal Challenge*

In April 1952, the bargaining procedures of the 1947 Taft-Hartley Act[99] failed to settle a dispute between the steel companies and their employees over the "terms and conditions that should be included in new collective bargaining agreements."[100] Consequently, the employees' representative, United Steelworkers of America, gave notice that the steelworkers would undertake a nationwide strike.[101] President Harry S. Truman responded to the impending strike by issuing an Executive Order directing the Secretary of Commerce to take possession of most of the steel mills and keep them running.[102]

Citing his own proclamation of "the existence of a national emergency" in the face of the United States's involvement in the Korean War in December 1950, President Truman's order asserted that steel was "indispensable" to U.S. national defense because of its centrality to military weapons and materials, Atomic Energy Commission programs, and the national economy.[103] Moreover, the Executive Order indicated that "a work stoppage would immediately jeopardize and imperil our national defense and the defense of those joined with us in resisting aggression, and would add to the continuing danger of our soldiers, sailors, and airmen engaged in combat in the field."[104] Ultimately, President Truman invoked his authority "by the Constitution and laws of the United States, and as President of the United States and Commander in Chief of the armed forces of the United States" to authorize and direct the Secretary of Commerce "to take possession of all or such of the plants, facilities, and other property of the companies named in the list attached hereto . . . as he may deem necessary in the interests of national defense" and to operate the steel companies or arrange for their operation.[105]

The Secretary of Commerce then issued his own orders, directing the steel company presidents to serve as operating managers for the United

---

[98] *Steel Seizure*, 343 U.S. at 589–90.
[99] 29 U.S.C. §§ 171–188 (2006).
[100] *Steel Seizure*, 343 U.S. at 582.
[101] *Id.* at 583.
[102] *Id.*
[103] *Id.* at 589–90.
[104] *Id.* at 590–91.
[105] *Id.* at 591.

States.[106] In response, the companies asked the U.S. District Court for the District of Columbia to declare the orders of the President and Secretary invalid and to issue injunctions restraining their enforcement.[107] The District Court granted a preliminary injunction against the Executive's seizure, but the Court of Appeals for the District of Columbia Circuit stayed the injunction, prompting the Supreme Court to grant certiorari.[108]

Six Justices agreed on the opinion of the Court, as delivered by Justice Black, that President Truman did not have the authority to issue the order. Four of the concurring Justices issued separate opinions; as Justice Frankfurter noted in his own concurrence, the five opinions authored by the majority Justices demonstrated "differences in attitude" sufficient to preclude "a single opinion for the Court."[109] The variety of constitutional approaches found in these opinions, along with a general sense that the Justices based their rulings heavily on the facts of this particular presidential action, makes it difficult to determine whether a future Executive, faced with an emergency of a different color, could rely on them as a legal basis for action against a private entity.

2. "An Act of Congress or from the Constitution Itself"[110]: Opinion of the Court

Justice Black's majority opinion framed the analysis as requiring presidential seizure authority to "stem either from an act of Congress or from the Constitution itself."[111] He rapidly ruled out the possibility that a statute or act of Congress had authorized President Truman to seize the steel mills.[112] Noting that the Government made no claim that express constitutional language gave the President authority to act, Justice Black moved on to the possibility that authority stemmed from "the President's military power as Commander in Chief of the Armed Forces" or "the several constitutional provisions that grant executive power to the President."[113]

---

[106] *Id.* at 583.
[107] *Id.*
[108] *Id.* at 584.
[109] *Id.* at 583 (Frankfurter, J., concurring).
[110] *Id.* at 585 (Frankfurter, J., concurring).
[111] *Id.*
[112] *Id.* at 585–86.
[113] *Id.* at 587.

Justice Black dismissed the notion that the Commander in Chief powers supported the seizure, drawing a contrast between "military commanders engaged in day-to-day fighting in a theater of war" and taking "possession of private property in order to keep labor disputes from stopping production."[114] Likewise, Justice Black dismissed the idea that the constitutional provisions granting Executive power permitted President Truman's action. The seizure, he contended, resembled a legislative enactment, as it set "out reasons why the President believes certain policies should be adopted, proclaim[ed] these policies as rules of conduct to be followed, and again, like a statute, authorize[d] a government official to promulgate additional rules and regulations consistent with the policy proclaimed and needed to carry that policy into execution."[115] Nothing in the Constitution subjected "this lawmaking power of Congress to presidential or military supervision or control," and this principle remained solid "even if other Presidents without congressional authority have taken possession of private business enterprises in order to settle labor disputes."[116]

3. "Could Not More Clearly and Emphatically Have Withheld Authority"[117]*: Justice Frankfurter's Concurrence*

Justice Frankfurter's concurring opinion opened with a declaration of fidelity to constitutional checks and balances and judicial minimalism, stressing a disinclination to delineate the full scope of presidential and congressional powers.[118] Turning to the facts at hand, Justice Frankfurter focused on two possible theories for finding President Truman's actions constitutional: their consistency with congressional action and their consistency with "systematic, unbroken, executive practice."[119] He concluded that neither theory sustained the seizure.

In assessing whether Congress's actions had authorized the President to act, Justice Frankfurter observed that Congress had "frequently—at least 16 times since 1916—specifically provided for Executive seizure of

---

[114] *Id.*
[115] *Id.* at 588.
[116] *Id.*
[117] *Id.* at 597–98 (Frankfurter, J., concurring).
[118] *Id.* at 597 (Frankfurter, J., concurring). Justice Frankfurter opined that the Court had an obligation to "avoid putting fetters upon the future by needless pronouncements today." *Id.* at 596.
[119] *Id.* at 610.

productions, transportation, communications, or storage facilities."[120] Justice Frankfurter surveyed these enactments and identified a set of common "limitations and safeguards" on the grants of power.[121] Justice Frankfurter then drew a contrast between this record of congressional enactments and Congress's intent regarding seizure of the steel industry. In debating the Taft-Hartley Act, Congress had rejected the idea that the Government would "[take] over property or [run] plants"[122] if a strike remained deadlocked, instead electing "not to make available in advance a remedy to which industry and labor were fiercely hostile."[123] Justice Frankfurter observed that Congress "presumably acted on experience with similar industrial conflicts" and had "evidently assumed that industrial shutdowns in basic industries are not instances of spontaneous generation, and that danger warnings are sufficiently plain before the event to give ample opportunity to start the legislative process into action."[124] He concluded that Congress "could not more clearly and emphatically have withheld authority than it did in 1947."[125]

Justice Frankfurter then dismissed the claim that consistency with past Executive practice rendered President Truman's actions constitutional. He acknowledged that Executive powers could extend beyond the text of Article II of the Constitution.

> [A] systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by Presidents who have sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on "executive

---

[120] *Id.* at 597–98.

[121] *Id.* at 587. Justice Frankfurter's summary of previous legislation involving executive seizure of private property, see *infra* Part IV.C.2.b, should represent, a starting point for policymakers creating legislation to address Executive action over private entities in the cybersecurity arena.

[122] *Id*. at 599 n.2 (Frankfurter, J., concurring) (quoting Senator H. Alexander Smith of the Senate Committee on Labor and Public Welfare).

[123] *Id.* at 601.

[124] *Id.* at 601–02. Justice Frankfurter characterized Congress's position as telling the President, "You may not seize. Please report to us and ask for seizure power if you think it is needed in a specific situation." *Id.* at 603.

[125] *Id.* at 597–98. Furthermore, Justice Frankfurter concluded that Congress had not altered its intent to deny the President seizure powers when it passed the Defense Production Act of 1950 or its 1951 Amendments to the Defense Production Act. *Id.* at 607–09.

Power" vested in the President by § 1 of Art. II.[126]

Nevertheless, President Truman's seizure of the steel mills did not correspond with any Executive practice deemed constitutional. Unlike the executive order withdrawing public lands from settlement in *United States v. Midwest Oil*,[127] the seizure order could not count on a lineage of presidential action "over a period of 80 years and in 252 instances."[128] President Lincoln's seizures of the railroads took place "in territory where armed hostilities had already interrupted the movement of troops to the beleaguered Capital," and Congress subsequently ratified the order.[129] President Wilson's and President Roosevelt's seizures of industrial facilities—with the exception of three pre-Pearl Harbor seizures by President Roosevelt that Justice Frankfurter quickly dismissed as "isolated" and unsanctioned—happened under congressional authority or after declaration of a state of war.[130] Because of the inapplicability of the various examples of prior Executive practice, Justice Frankfurter concluded that Article II, both in text and application, failed to support President Truman's seizure.

4. "A Taking in the Constitutional Sense"[131]*: Justice Douglas' Concurrence*

Justice Douglas viewed President Truman's action as a condemnation of property—a "taking in the constitutional sense."[132] He rested his conclusion of unconstitutionality on the theory that Congress, as the only branch of the U.S. Government with the power to compensate a private party for a seizure of property, was the sole entity able to "authorize a seizure or make lawful one that the President has effected."[133] While Justice Douglas's concurrence resolved the case with a simpler approach than the other concurrences, it did offer, in footnotes, two observations with the potential to cloud matters in a future national security controversy. First, he noted that "[w]hat a President may do as a matter of expediency or extremity may never reach a definitive

[126] *Id.* at 610–11.
[127] 236 U.S. 459 (1915).
[128] *Steel Seizure*, 343 U.S. at 611 (Frankfurter, J., concurring).
[129] *Id.*
[130] *Id.* at 611–13.
[131] *Id.* at 631 (Douglas, J., concurring).
[132] *Id.*
[133] *Id.* at 631–32.

constitutional decision."[134] He further observed that "[w]artime seizures by the military in connection with military operations . . . are also in a different category."[135]

5. "A Poverty of Really Useful and Unambiguous Authority"[136]*: Justice Jackson's Concurrence*

Of the Justices in the *Steel Seizure* majority, Justice Jackson seemed the most interested in providing a framework for evaluating the constitutionality of future Executive action, rather than merely evaluating the facts before him.[137] Alluding to his own service as a government attorney during the administration of President Franklin D. Roosevelt, Justice Jackson opened the opinion by acknowledging that Supreme Court precedent provided a "poverty of really useful and unambiguous authority applicable to concrete problems of executive power as they actually present themselves."[138] He then identified a "somewhat over-simplified grouping" of three types of situations involving presidential decision-making.[139]

The first situation would involve a President who "acts pursuant to an express or implied authorization of Congress"; with this type of authorization, presidential authority would be "at its maximum."[140] Justice Jackson observed that, if the Court viewed action under congressional authorization unconstitutional, "it usually means that the Federal Government as an undivided whole lacks power."[141]

The second situation involving presidential decision-making would

---

[134] *Id.* at 631 n.1.
[135] *Id.* at 631 n.2.
[136] *Id.* at 634 (Jackson, J., concurring).
[137] Whether Justice Jackson did, in fact, provide a useful framework remains open for debate. *See* Neal Kumar Katyal, Hamdan v. Rumsfeld*: The Legal Academy Goes to Practice*, 120 HARV. L. REV. 65, 99 (2006) (asserting that "Youngstown's framework has become the gold standard, perhaps because its all-things-to-all-people quality can provide arguments favoring any branch of government under many circumstances").
[138] *Steel Seizure*, 343 U.S. at 634 (Jackson, J., concurring).
[139] *Id.* at 635.
[140] *Id.*
[141] *Id.* at 636. The Supreme Court's ruling in *Clinton v. City of New York*, 524 U.S. 417 (1998), holding the Line Item Veto Act unconstitutional even though both Congress and the President had supported it is an example of this. *See* Robert J. Reinstein, *The Limits of Executive Power*, 59 AM. UNIV. L. REV. 259, 261 n.5 (2009).

occur when "the President acts in absence of either a congressional grant or denial of authority."[142] According to Justice Jackson, this balance would implicate a "zone of twilight in which [the President] and Congress may have concurrent authority, or in which its distribution is uncertain."[143] The constitutionality of Executive action would be heavily dependent on the facts and circumstances of a given situation: "[A]ny actual test of power is likely to depend on the imperatives of events and contemporary imponderables rather than on abstract theories of law."[144]

Finally, Justice Jackson observed that presidential power would be at its lowest when it involves "measures incompatible with the expressed or implied will of Congress."[145] Courts could find such presidential actions constitutional "only by disabling the Congress from acting upon the subject."[146] Reviewing the facts of President Truman's seizure, Justice Jackson concluded that it fit into the third category, sustainable "only by holding that seizure of the strike-bound industries is within [the President's] domain and beyond control by Congress."[147] He further concluded that none of the relevant constitutional clauses, nor prior presidential practices, supported a finding of constitutionality.[148] While addressing the Solicitor General's argument that the constitutional clause designating the president as Commander in Chief authorized the seizure, Justice Jackson indicated that he would "indulge the widest latitude of interpretation to sustain [the President's] exclusive function to command the instruments of national force, at least when turned against the outside world for the security of our society."[149] Instances involving "a lawful economic struggle between industry and labor," by contrast, did not warrant such judicial discretion.[150] Consequently, Justice Jackson regarded President Truman's steel seizure an appropriate instance for judicial intervention.[151]

---

[142] *Steel Seizure*, 343 U.S. at 637 (Jackson, J., concurring).
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.* at 637–38.
[147] *Id.* at 640.
[148] *Id.* at 640–51.
[149] *Id.* at 645.
[150] *Id.*
[151] Justice Burton and Justice Clark also filed concurrences, expressing views similar to the other concurring Justices. Justice Burton focused his concurrence on the seizure's incompatibility with the Labor Management Relations Act, noting that "the most significant feature of that Act is its omission of authority to seize an affected industry." *Id.* at 657 (Burton, J., concurring). As with several of the other concurrences, Justice

6. "Arguments Favoring Any Branch of Government Under Many Circumstances"[152]*: Applying* Steel Seizure *to Cybersecurity Emergencies*

While the Justices evaluating President Truman's seizure of the steel industry laced their opinions with dicta sufficient to fuel generations of debate over a wide variety of Executive actions,[153] the opinions ultimately leave the Executive Branch and other legal practitioners without clear guidance on how federal courts would handle a challenge to Executive action in the face of a cybersecurity emergency. A significant weakness limits *Steel Seizure*'s predictive value in a cybersecurity case: the legislative history, a primary focus of the Justices in *Steel Seizure*, would be dramatically different. *Steel Seizure* represents an instance of Executive action following an explicit congressional decision to deny the Executive that action.[154] Because Congress has never expressly declined to grant the Executive powers over private entities in the event of a cybersecurity emergency, the legislative history aspect of the majority opinion and concurrences—probably the greatest area of agreement among the concurring Justices—would not apply to a cybersecurity case. This difference would diminish much of *Steel Seizure*'s precedential value.

In a case with such materially different facts from *Steel Seizure*, the bulk of legal arguments, from the Executive side and other interested parties alike, would revolve around *Steel Seizure*'s dicta about Executive authority. If required to justify a seizure of privately owned hardware, the Executive Branch would probably rely on the suggestion, on the part of several of the Justices, that *Steel Seizure*'s outcome in a case of

---

Burton's concurrence indicated that the Court was not ruling on the President's powers in the face of "imminent invasion or threatened attack." *Id.* Justice Clark likewise found the seizure unconstitutional on the grounds that "Congress had prescribed methods to be followed by the President in meeting the emergency at hand" in the Labor Management Relations Act, Defense Production Act of 1950 and Selective Service Act of 1948. *Id.* at 662 (Clark, J., concurring). He stressed that the case was not controlling for all future presidential action, indicating that "in the absence of such action of Congress, the President's independent power to act depends upon the gravity of the situation confronting the nation." *Id.*

[152] Katyal, *supra* note 137, at 99.

[153] *See, e.g.*, Massachusetts v. Laird, 400 U.S. 886 (1970) (constitutionality of the United States' participation in the Vietnam War); Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 500 (1977) (Powell, J, concurring) (whether a recently-resigned President Nixon could retrieve his presidential papers from the U.S. Government); Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (amount of due process owed an "enemy combatant" post-September 11, 2001).

[154] *See supra* notes 119–125 and accompanying text.

"armed attack or imminent invasion" might have been different.[155] In response, a party opposing Executive action might cite Justice Frankfurter's attempt to find an unbroken lineage of Executive practice and claim that none existed under the circumstances. As Professor Neal Kumar Katyal has observed, Justice Jackson's opinion in *Steel Seizure*—featuring the closest that the majority Justices come to a principle of general applicability—suffers "perhaps because its all-things-to-all-people quality can provide arguments favoring any branch of government under many circumstances."[156] Given this precedential terrain, it is impossible to predict how a federal court would rule, if faced with a challenge to Executive action.

Moreover, *Steel Seizure*'s dicta provide, at best, only a basis for Executive action. They provide an even shakier foundation for divining the limitations or details of Executive power. The amount of compensation for a private party that loses revenue as a result of an Executive-mandated shutdown of its hardware, for example, would have to be determined through some other means. With *Steel Seizure* as guidance, future legal conflicts over cybersecurity would be mired in Justice Jackson's "zone of twilight."

B. Other Sources of Executive Authority Over Private Parties: National Defense Areas

Without case law or statutes to bestow the Executive Branch with

---

[155] Commentators have regarded *Youngstown Sheet & Tube Co*. as providing room for Executive action against national emergencies.

> Although Steel Seizure seems to reject the existence of any executive emergency power, a careful examination of all seven opinions filed does not support such a definitive assertion. An analysis of the concurring and dissenting opinions indicates that a majority of the justices embraced the existence of some residual presidential emergency power. They divided on the question whether Congress nonetheless had implied prohibited the President's conduct. Moreover, despite the government's argument and President Truman's statement, no emergency existed. Ample time existed for congressional action, both before and after the seizure, yet Congress did nothing. To transform political deadlock into an emergency would drain the concept of emergency of all content.

Monaghan, *supra* note 91, at 37–38.

[156] *See* Katyal, *supra* note 137, at 99.

unambiguous authority over the private entities comprising cyberspace, a President seeking to respond to a cybersecurity crisis could next turn to regulations and practices for a source of legal authority. Department of Defense (DoD) regulations recognize the authority of military commanders to establish "National Defense Areas" (NDA) to protect military installations, property and personnel. Department of Defense Directive 5200.8, *Security of DoD Installations and Resources*,[157] a regulation promulgated in 1991, stands as the highest-level articulation of the NDA concept.

Department of Defense Directive 5200.8 indicates that the "authority of a DoD installation commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property" includes "temporarily established 'National Defense Areas' under emergency situations such as accident sites involving federal equipment or personnel on official business."[158] The relevant service regulations do not address compensation for affected private entities, but the Air Force's summary of guidance to military commanders, *The Military Commander and the Law*, indicates that "[b]ecause the NDA effectively deprives the landowner of the use of the property during the period the NDA is in existence, the Air Force may have to compensate the landowner for the temporary 'taking' of the property."[159]

The lack of written legal authority[160]—and a severe limitation on the Executive Branch's use of NDAs as a coercive tool in cybersecurity emergencies—is a product of the DoD's practice of generally invoking the NDA principle under relatively uncontroversial circumstances, free of the complicating presence of large sums of money, potential abridgement of free expression, or other contentious matters. Ordering the shutdown of a private entity's Internet hardware, by contrast, would be more likely to implicate those sorts of sensitive issues. While the

---

[157] U.S. DEP'T OF DEF., DIR. 5200.8, SECURITY OF DOD INSTALLATIONS AND RESOURCES (Apr. 25, 1991).

[158] *Id.* para. 3.2; *see also* Richard Ripley, *Jackknifed Truck Carrying Missile Has Been Secured*, THE SPOKESMAN-REV., Oct. 31, 1985, at A6 (describing Air Force declaration of "National Defense Area" after a vehicle carrying a nuclear cruise missile jack-knifed and went off of the highway in Oregon).

[159] AIR FORCE JUDGE ADVOCATE GEN.'S SCHOOL, THE MILITARY COMMANDER & THE LAW 390 (2009), http://milcom.jag.af.mil/Military_CC_and_Law_2009.pdf.

[160] A search of the LEXIS "Federal Courts" database revealed no published opinions addressing the extent or limitations of the DoD's power to establish and maintain National Defense Areas (NDAs).

DoD's recent establishment of chains of command over cyberspace operations[161] raises the possibility that a commander could declare an NDA over affected private hardware, this application stands to stretch the NDA concept too far. The NDA regime would almost certainly lack the nuance necessary to handle the full array of issues arising in a cybersecurity emergency.

Ultimately, the current state of the legal authority that might allow the Executive Branch to impose its authority over the sort of hijacked private server used by Georgia's cyberattackers in July 2008 is uncertain and ambiguous. While a 2009 *Air Force Law Review* article on cyberneutrality asserted that the "U.S. Constitutional framework is more than adequate to allow for appropriate action" to enforce America's cyberneutrality, the article focused on national security doctrine—not on the Executive Branch's legal authority for coercive action against a reluctant private entity.[162] Under these circumstances, all relevant interests would best be served by legislation that clearly establishes Executive authority and procedures.

IV. The Cybersecurity Act of 2009: Empowering the Executive Response?

A. "Maintain Effective Cybersecurity Defenses Against Disruption"[163]: Senator Rockefeller's Initial Proposal

On April 1, 2009, Senator Rockefeller attempted to address the void of legal authority described in Part III of this article by introducing Senate Bill 773, the "Cybersecurity Act of 2009."[164] Co-sponsored by three senators—two Democrats and one Republican—the bill aimed to

---

[161] *See* Thom Shanker, *New Military Command for Cyberspace*, N.Y. TIMES, June 23, 2009, *available at* http://www.nytimes.com/2009/06/24/technology/24cyber.html (indicating that Robert M. Gates, the Secretary of Defense, had "ordered the creation of the military's first headquarters designed to coordinate Pentagon efforts in the emerging battlefield of cyberspace and computer-network security").

[162] Kastenberg, *supra* note 12, at 57.

[163] Cybersecurity Act of 2009, S. 773, pmbl., 111th Cong. (2009).

[164] Cybersecurity Act of 2009, S. 773, 111th Cong. (2009); *see also* Kastenberg, *supra* note 12, at 49 (discussing S. 773). On the same day, Senator Rockefeller also introduced Senate Bill 778, a bill establishing the office of National Cybersecurity Advisor within the Executive Office of the President. To Establish, Within the Executive Office of the President, the Office of the National Cybersecurity Advisor, S. 778, 111th Cong. (2009). (Notwithstanding S. 778, President Barack H. Obama appointed Howard Schmidt as the

> ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications, to provide for the continued development and exploitation of the Internet and intranet communications for such purposes, to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption.[165]

The bill's "Findings" section identifies "America's failure to protect cyberspace" as "one of the most urgent national security problems facing the country."[166] To support this assertion, the section then cites a series of authorities—both governmental and private sector—on the United States' lack of readiness to face potential cyberthreats and the potential consequences that could result from such an attack.[167]

The bill proposed a series of measures to address cyberthreats. Section 3 envisions a "Cybersecurity Advisory Panel" to "advise the President on matters relating to the national cybersecurity program and strategy."[168] Section 6 tasks the National Institute of Standards and Technology with "establish[ing] measurable and auditable cybersecurity standards for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks."[169] Section 7 mandates that the Secretary of Commerce "develop or coordinate and integrate a national licensing, certification, and periodic recertification program for cybersecurity professionals."[170]

White House Cybersecurity Coordinator in December 2009. Ellen Nakashima & Debbi Wilgoren, *Obama Names Howard Schmidt as Cybersecurity Coordinator*, WASH. POST, Dec. 22, 2009, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/12/21/AR2009122103055.html).

[165] S. 773, pmbl.

[166] *Id.* § 2(1).

[167] *Id.* § 2. For example, Finding (3) quotes the 2009 Annual Threat Assessment for the proposition that "a successful cyberattack against a major financial service provider could severely impact the national economy, while cyberattacks against physical infrastructure computer systems such as those that control power grids or oil refineries have the potential to disrupt services for hours or weeks." *Id.* § 2(3).

[168] *Id.* § 3.

[169] *Id.* § 6.

[170] *Id.* § 7.

Section 18 provoked the most controversy.[171] The section assigns a list of "Cybersecurity Responsibilities and Authorities" to the President.[172] In paragraph (2), the bill indicates that the President "may 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."[173] In paragraph (6), the bill states that the President "may order the disconnection of any Federal Government or United States critical infrastructure information systems or networks in the interest of national security."[174]

Essentially, this language proposes giving the President two tools: "limitation or shutdown" in the event of a "cybersecurity emergency" and "disconnection" in "the interest of national security." The bill includes a "Definitions" section in Section 23 but does not include definitions of "limitation or shutdown," "cybersecurity emergency," "disconnection," or "interest of national security."[175] It does, however, provide a definition of "Federal Government and United States critical infrastructure information systems and networks," namely, "Federal Government information systems and networks" and "State, local, and nongovernmental information systems and networks in the United States designated by the President as critical infrastructure information systems and networks."[176]

B. "In Coordination with Relevant Industry Sectors"[177]: Reported Changes

Five months later, CNET News reported that Senator Rockefeller's staff had drafted a revised bill.[178] The reported revision replaces the controversial language of Section 18, paragraph (2), with new language.[179] The new language specifies a precondition to presidential

---

[171] *See* McCullagh, *supra* note 30.
[172] S. 773 § 18.
[173] *Id.* § 18(2).
[174] *Id.* § 18(6).
[175] *Id.* § 23.
[176] *Id.*
[177] McCullagh, *supra* note 30, at 244.
[178] *See id.*; *see also* Brown, *supra* note 23, at 244 (discussing reported changes to the Cybersecurity Act).
[179] *See* McCullagh, *supra* note 30.

action: "in the event of an immediate threat to strategic national interests involving compromised Federal Government or United States critical infrastructure information system or network."[180] If that precondition arises, the President could "declare a cybersecurity emergency" and, "if [he or she] finds it necessary for national defense and security, and in coordination with relevant industry sectors, direct the national response to the cyber threat and the timely restoration of the affected critical infrastructure information system or network."[181]

The draft revision alters the paradigm of presidential action in the face of a cybersecurity emergency. In the original version, the President would act unilaterally—limiting, shutting down, or disconnecting the Internet, without any coordination or input from the private sector. The revised version contemplates a more cooperative Executive response; the presidential action would be "in coordination with relevant industry sectors."

C. Strengths and Weaknesses of the Proposed Cybersecurity Act

1. Strengths of the Proposed Cybersecurity Act

Senator Rockefeller's proposed Cybersecurity Act—in both incarnations—represents a significant improvement over the current state of the law, but it still suffers from substantial weaknesses. By establishing a legal basis for Executive Branch authority over private entities in a cybersecurity emergency, it will allow the Executive to bypass the obstacle of persuading the courts and the American public that the Justices' various pronouncements in *Steel Seizure* grant authority to the Executive. As the initial response to the proposal suggests,[182] some percentage of the American public will be uncomfortable with the idea of giving the Executive Branch this power in the first place. Certainly, the proposed system does not completely preclude the possibility of politically motivated abuse, such as a President invoking the Cybersecurity Act to shut down the Internet access of an administration critic. Nevertheless, the likelihood of cyberattack and the potentially severe consequences of such an attack suggest that the most prudent approach would be to craft legislation granting power to the Executive

---

[180] *Id.*
[181] *Id.*
[182] *See id.*

Branch, along with an oversight mechanism to check that power.

Moreover, the proposed Cybersecurity Act gives the Executive Branch the operational tools necessary to respond to the cybersecurity crises described in this article. In authorizing the President to shut down an affected portion of the Internet or limit traffic, Senator Rockefeller's initial proposal would allow an appropriate Executive Branch response to the DDOS attack against Georgia in July 2008, where shutting down an unwittingly hijacked privately-owned server effectively halted the attack. It would also provide the Executive Branch with a means of stopping Internet activity when that activity jeopardizes an official position of neutrality. While the reported change would replace the specifically enumerated measures of the initial proposal with more general "direct the national response" language, the Executive Branch may be able to interpret that language to include shutting down or limiting an affected portion of the Internet in the President's options.[183]

2. Weaknesses of the Proposed Cybersecurity Act

While Senator Rockefeller's proposed Cybersecurity Act offers substantial advantages over the legal regime currently governing Executive Branch actions in cybersecurity emergencies, the bill also has several shortcomings. Its lack of an oversight mechanism is its greatest weakness, especially in light of Supreme Court opinions that have regarded Executive actions under similar statutes as falling outside the purview of judicial review. Moreover, the bill leaves several significant aspects of its implementation undefined or vague. This article recommends rewriting the Cybersecurity Act to improve these deficiencies.

a. "Reviewability"[184]*:* Dakota Central *and Judicial Deference to Executive Decision-Making*

The likelihood that Executive Branch action in a cybersecurity

[183] Ultimately, a conclusive analysis of this aspect of the proposal will be impossible until the bill has been debated in Congress, which would provide an indication of congressional intent.

[184] Kevin M. Stack, *The Reviewability of the President's Statutory Powers*, 62 VAND. L. REV. 1171, 1173 (2009).

emergency would affect substantial domestic interests, such as commerce or free expression, renders an oversight mechanism necessary.[185] A line of Supreme Court opinions suggests, however, that Senator Rockefeller's proposal would bar judicial review of any Executive actions that it authorizes. Both versions of the Cybersecurity Act of 2009 require the President to make certain determinations—for example, declaring that a situation represents a "cybersecurity emergency"—as a predicate to action. When evaluating the constitutionality of statutes imposing similar requirements on the Executive Branch as a precondition to action, the Supreme Court has consistently invoked a "reviewability" doctrine and declined to review whether the President had properly invoked his statutory powers, thereby precluding review of the challenged action.[186]

This judicial doctrine stems from a case involving a challenge to presidential action under a statute with similarities to both versions of the Cybersecurity Act. In 1919, the Supreme Court decided *Dakota Central Telephone Co. v. South Dakota*, a case that featured a challenge to the President's authority under a World War I joint resolution.[187] A year earlier, Congress had adopted a joint resolution authorizing the President "during the continuance of the present war . . . whenever he shall deem it necessary and for the national security or defense, to supervise or take possession and assume control of any telegraph [or] telephone . . . cable," provided just compensation was given.[188]

President Woodrow Wilson used this grant of authority in July 1918 to take possession of all telephone and telegraph systems; he then delegated the supervision of the systems to the Postmaster General.[189] The signing of the Armistice on November 11, 1918, ended World War I. Nevertheless, the Postmaster General, acting pursuant to the President's delegation, issued an order on December 18 increasing the

---

[185] Although the United States does not subject every single one of its national security decisions to a direct oversight regime, few national security decisions implicate significant domestic interests to the same extent as Executive Branch intervention in cybersecurity matters. Consequently, a prudent legal regime in this area would include some measure of direct oversight.

[186] Stack, *supra* note 184 ("[T]his doctrine operates to exclude judicial review of the determinations or findings the President makes to satisfy conditions for invoking grants of statutory power.").

[187] Dakota Cent. Tel. Co. v. South Dakota, 250 U.S. 163 (1919).

[188] *Id.* at 181 (quoting joint resolution of July 16, 1918, 40 Stat. 904).

[189] *Id.* at 182–83 (quoting President Wilson's proclamation of July 22, 1918).

rates for intrastate calls in South Dakota.[190]

The State of South Dakota responded to the order by seeking an injunction against the Postmaster General.[191] South Dakota contended that the end of the war had quashed any conceivable connection between the intrastate phone rates and national security, thereby eliminating the Executive Branch's authority to set call rates under Congress's resolution.[192] The Court declined to review South Dakota's challenge to the President's authority on the grounds that "the contention at best concerns not a want of power, but a mere excess or abuse of discretion in exerting a power given, it is clear that it involves considerations which are beyond the reach of judicial power."[193]

The Court further indicated that "the judicial may not invade the legislative or executive departments so as to correct alleged mistakes or wrongs arising from asserted abuse of discretion."[194] As a commentator emphasized in a 2009 law review article, "[o]n this logic, it is difficult to imagine a circumstance in which a court would review whether the President's assertion of authority exceeded the power given."[195] While the enactment of the Administrative Procedure Act (APA) eliminated that exclusion from review for most Executive officials, the Supreme Court has held that the APA does not apply to the President.[196] Consequently, courts have continued to apply the reviewability doctrine in suits challenging the President's claims of statutory power.[197]

A shutdown or limitation of Internet use under the Cybersecurity Act will most likely implicate significant economic and free expression interests. As noted above, the proposed legislation grants the Executive Branch powers that a President could abuse, for example, to silence an administration critic. In this context, the *Dakota Central* line of precedent creates a significant shortcoming for Senator Rockefeller's proposal. If a private entity were to challenge an executive order, issued pursuant to the Cybersecurity Act, to shut down its server, the President's finding of a "cybersecurity emergency" or the "interests of

---

[190] Stack, *supra* note 184, at 1185.
[191] *Dakota Cent. Tel. Co.*, 250 U.S. at 179.
[192] Stack, *supra* note 184, at 1185.
[193] *Dakota Cent. Tel. Co.*, 250 U.S. at 184.
[194] *Id.*
[195] Stack, *supra* note 184, at 1186.
[196] *Id.* at 1173.
[197] *Id.*

national security" under the initial version, or a "cybersecurity emergency" under the second version, would serve to foreclose further judicial review. Part V, below, will discuss oversight mechanisms capable of improving this deficiency.

b. Consistency with Previous Seizure Legislation: Justice Frankfurter's Checklist

Justice Frankfurter's concurrence in *Steel Seizure*[198] summarized previous congressional legislation empowering the Executive Branch to conduct seizures in certain industries. Specifically, Justice Frankfurter noted that Congress had consistently granted the power to seize "for a limited time or for a defined emergency" or "repealed [the power] after a short period," consistently restricted the circumstances in which the President could exercise the power, imposed limitations on the period of governmental operation under the power, made Executive action dependent on specific conditions, specified the particular Executive agency entrusted with the power, and "legislated in detail" on potential compensation payment.[199] Concededly, Justice Frankfurter prepared his summary to contrast the circumstances of previous constitutionally sanctioned seizures with President Truman's unauthorized actions; his purpose was not to provide a controlling template for future legislators. Nevertheless, to ensure that any proposed cybersecurity legislation remains consistent with a judicially approved legislative tradition, Congress should draft the legislation with Justice Frankfurter's "checklist" in mind.

In general, Senator Rockefeller's proposal satisfies Justice Frankfurter's criteria. The Cybersecurity Act as drafted, either on its face or through a reasonable interpretation of legislative intent, suggests that it creates a grant of power for a defined emergency that is applicable under restricted circumstances and for a limited period of time, that is entrusted to a specific federal official, and that depends on specific conditions. All of these limitations presume the President has acted legitimately and refrained from abusing his ability to declare a cybersecurity emergency under the statute. To best address that concern, however, Congress could incorporate an oversight mechanism, especially since the "reviewability" doctrine stands to preclude judicial review.

---

[198] *See supra* Part III.A.3.
[199] *Steel Seizure*, 343 U.S. 579, 598 (1952) (Frankfurter, J., concurring).

The proposal does omit one item identified in Justice Frankfurter's survey of its antecedents: the detailed description of how the government will compensate a private entity whose property is seized under the Cybersecurity Act. An Executive dictate to shut down or limit Internet use stands to cause financial harm to a private entity with a hijacked server. Given the amount of commerce traversing the Internet, the dollar value of such harm could be astronomical.[200] Consequently, a system for compensating disadvantaged private entities should be an essential requirement in a forward-looking legal regime addressing Executive Branch action in cybersecurity emergencies.

c. Other Weaknesses

Several other areas of the proposed Cybersecurity Act are concerning. Overall, the bill suffers from many undefined terms. In the reported changes, for example, the statute leaves unanswered the identity of "relevant industry sectors," the amount and quality of coordination necessary to satisfy the statute, and the specifics on handling decision-making if the President disagrees with industry or industry sectors lack consensus. All these aspects of an Executive Branch response to a cybersecurity emergency under the Act could be contentious. The Act, when enacted, should provide a framework to handle these contingencies.

Moreover, neither version of the Act explicitly includes the compromise of U.S. neutrality as the sort of national security emergency that would allow the President to take action under the Act. As discussed above,[201] a private entity's actions in cyberspace that jeopardize a United States position of neutrality could have serious consequences that trigger a national security emergency, requiring the President to take action under the Cybersecurity Act. The Cybersecurity Act should explicitly define the compromise of the United States' neutrality as a "cybersecurity emergency" to ensure that the Executive Branch will be able to act without question in these circumstances.

---

[200] *See* COLARIK, *supra* note 38.
[201] *See supra* Part II.C.

V. Proposed Oversight Regime for Empowering Executive Branch Against Cyberemergencies

As discussed in Part IV, Senator Rockefeller's proposed legal regime for Executive Branch action in cybersecurity emergencies represents a significant improvement over the current state of the law, but it suffers from significant weaknesses. The most significant weakness, in light of the domestic interests at stake in a shutdown or limitation of Internet use, is its lack of an oversight regime.[202] To correct this deficiency, this article proposes borrowing an oversight regime from another national security arena. In the 1970s, the United States developed two legal regimes for oversight of Executive Branch actions involving national security. The first became law in 1973 when Congress passed the War Powers Resolution[203] over President Richard M. Nixon's veto. The second is the Foreign Intelligence Surveillance Act of 1978 (FISA).[204] Including an oversight mechanism in the Cybersecurity Act similar to the War Powers Resolution or FISA would ease concerns that *Dakota Central* and its progeny would allow Executive discretion under the Act to stand unchecked and unbalanced.

A. The War Powers Resolution

The first option would be a regime similar to the War Powers Resolution. Passed in the aftermath of the United States' involvement in Vietnam, the War Powers Resolution is Congress's primary means of oversight for the use of the U.S. Armed Forces in combat.[205] The most significant aspect of the War Powers Resolution for cybersecurity legislation purposes is section 1543, which requires the President to report to Congress if military force is used abroad.[206]

---

[202] *See supra* Part VI.C.2.a.

[203] 50 U.S.C §§ 1541–1548 (2006). For a more thorough discussion of the War Powers Resolution and its application to American military involvement, see generally Michael Mandel, *A License To Kill: America's Balance of War Powers and the Flaws of the War Powers Resolution*, 7 CARDOZO PUB. L. POL'Y & ETHICS J. 785 (2009).

[204] Originally enacted as the Foreign Intelligence Surveillance Act of 1978 (FISA), Pub. L. No. 95–511, §§ 103, 104(a)(7)(A)–(C), 92 Stat. 1783, 1788–89 (1978) (codified as amended at 50 U.S.C. §§ 1801– 1863 (2006)).

[205] 50 U.S.C § 1541(a).

[206] *Id.* § 1543. The War Powers Act also includes a requirement, in § 1542, that the President must "consult" with Congress before force is used and for the duration of such hostilities. *Id.* § 1542. Commentators contend that this provision's lack of specificity has rendered it essentially unenforceable. Mandel, *supra* note 203, at 790.

If the President introduces U.S. Armed Forces "into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances," section 1543 requires the President to submit a written report to Congress within forty-eight hours, detailing "the circumstances necessitating the introduction of . . . Armed Forces; . . . the constitutional and legislative authority under which such introduction took place; and . . . the estimated scope and duration of the conflict."[207] Subsequently, the President must submit additional reports to Congress at least once every six months.[208] The final element of the War Powers Resolution's check on Executive power comes in section 1544, which requires the President to withdraw or terminate use of military forces within a sixty-day window after the initial report, unless Congress specifically authorizes their continuing presence through a declaration of war or a specific resolution, or is physically unable to meet because of an armed attack against the United States.[209]

B. The Foreign Intelligence Surveillance Act of 1978

Congress could also opt for an oversight regime borrowing from the FISA. The FISA became law in 1978 in response to concerns, prompted by the Watergate scandal and the Church Committee's study of domestic surveillance,[210] about the need for increased oversight of the Executive Branch's use of electronic surveillance.[211] The central premise of the FISA was a compromise between national security and civil liberties aims: "authorizing secret electronic surveillance for the purpose of collecting foreign intelligence, but subjecting applications to judicial scrutiny and the entire process to congressional oversight."[212] The main mechanism for achieving that purpose was a special court, the Foreign Intelligence Surveillance Court (FISC), meeting in secret, *ex parte*.[213]

The FISC procedure imposes a series of safeguards on the Executive

---

[207] 50 U.S.C § 1543.
[208] *Id.*
[209] *Id.* § 1544; Mandel, *supra* note 203, at 791.
[210] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94–755 (1976).
[211] *See generally* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1216–28 (2007) (providing a detailed discussion of the historical context for FISA's passage).
[212] *Id.* at 1214–15.
[213] 50 U.S.C § 1803(a)(2).

Branch before it can conduct electronic surveillance. Applications to the FISC require cabinet-level approval and certification of the surveillance's primary purpose.[214] Only the judge determining the lawfulness of the surveillance can review the evidence.[215] The FISA prescribed time limits for the surveillance, with opportunities for the Government to request extensions.[216]

The scheme also provided for vigorous Executive action. The FISA dictated that the FISC judge "shall" issue the surveillance order upon making the required statutory findings.[217] The law included several limited-but-significant exceptions to the FISA process, including a provision permitting the Attorney General to certify that "an emergency situation exists," requiring electronic surveillance before an order from the FISC can be obtained.[218] Under this emergency authority, the Executive Branch may conduct surveillance for up to seventy-two hours from the time the Attorney General requests authorization until it obtains the information sought or until the FISC denies the application for surveillance, whichever is earlier.[219] The Executive Branch must submit an application to a judge under the emergency exception, but it is not required until seventy-two hours after the emergency authorization.[220]

C. Oversight Proposal

The War Powers Resolution and FISA offer examples of oversight regimes that Congress could incorporate into the Cybersecurity Act to serve as a check against Executive action. In over three decades of experience with both regimes, FISA has proven the more workable of the two, which suggests that it would be a superior model for the Cybersecurity Act.[221] A cybersecurity oversight regime borrowing from

---

[214] *Id.* § 1805(a) (approval by Attorney General); *id.* § 1804(a)(7)(B) (current version at 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2003)) (certification requirement prior to amendment by USA PATRIOT Act in 2001).
[215] *Id.* § 1806(f).
[216] *Id.* § 1805(e).
[217] *Id.* § 1805(a).
[218] *Id.* § 1805(f)(1).
[219] *Id.* § 1805(f).
[220] *Id.*
[221] For a suggestion that a FISA-like regime be instituted to provide oversight in another national security area, see James Kitfield, *Predators*, NAT'L J. (Jan. 9, 2010), *available at* http://www.nationaljournal.com/njmagazine/cs_20100109_8396.php (application of FISA-like procedure to government program of targeted assassination of terrorists).

the FISA could facilitate a vigorous Executive Branch response to a cybersecurity emergency by allowing the Executive to present evidence justifying the Internet shutdown or limitation in secret, while allowing an emergency exception when especially prompt action is warranted. This regime could also uphold an appropriate balance between individual liberty and national security interests by ensuring that the Executive Branch would have to articulate its reason for an Internet shutdown or limitation, swear to the rationale under penalty of perjury, and persuade a judge that a cybersecurity emergency exists. Moreover, a regime with judicial oversight could also include a system for determining the amount of compensation the United States would owe to a private party suffering financial harm from Executive Branch actions in response to a cybersecurity emergency. This oversight regime would represent a substantial improvement over the proposed Cybersecurity Act.

VI. "Some Awful Calamity That Validates the Importance of the Threat"[222]: Conclusion

Because of the potentially immense consequences of a cyberattack or of a private individual's actions that compromise the nation's neutrality, the Executive Branch of the U.S. Government must be empowered to respond effectively to emergencies involving the nation's governmental and commercial cyberinfrastructure. The current state of the law provides neither definite authority nor useful limitations on that authority. Consequently, legislation defining Executive powers and specifying checks against those powers is essential.

While Senator Rockefeller's proposed Cybersecurity Act of 2009 improves the current state of the law by establishing an indisputable basis for Executive action, the Act, in both of its proposed versions, provides an inadequate legal regime. As *Dakota Central* and its progeny indicate, the Supreme Court's "reviewability" doctrine would mean that any courts reviewing challenged actions would defer to the Executive completely. In most circumstances requiring the President to invoke the Cybersecurity Act, the issue of coerciveness probably would be academic. Most likely, a U.S.-based company that learned that cyberattackers were using its hardware for an assault against the United States' governmental or commercial cyberinfrastructure would take the necessary measures to stop the attack, as the private owner of the server

[222] RICHARD A. CLARKE, AGAINST ALL ENEMIES 238–39 (1st trade paperback ed. 2004).

used in the July 2008 cyberattack on the Georgian infrastructure did. Controversy, if it existed, would probably be over whether the U.S. Government compensated the company for the seizure and, if so, how much compensation would be owed.

It is conceivable, however, that a private entity whose hardware has been hijacked might object to a seizure. This might happen if the private entity disputes that it is the gateway of an attack, or, more likely, if it were willingly compromising U.S. neutrality by assisting a sympathetic foreign power in an international conflict. In both cases, the Executive Branch would need coercive powers over the private entity to halt the attacks. By providing an oversight regime drawn from the War Powers Resolution or FISA, the improved Cybersecurity Act proposed in this article would allow for a check on the Executive while still allowing for a rapid response to cyberattacks or conduct that compromises neutrality and results in a national security emergency. Moreover, the regime would also provide a means for determining appropriate compensation for the seizure of private equipment.

Certainly, the relatively recent emergence of cyberwarfare explains one of the main difficulties in devising a legal regime for cybersecurity.[223] Legal regimes generally develop in response to real-world occurrences and aim to put policymakers in a better position than in an earlier crisis. Nevertheless, because of the potentially severe

---

[223] In this respect, cyberwarfare is similar to another nascent variety of warfare: space warfare. As Robert A. Ramey indicated in the *Air Force Law Review*,

> [T]he legal analysis of issues unique to space combat . . . cannot rely solely on analogy with legal relationships governing other combat environments. This is due in part to the relative infancy of space warfare and to the recency of its technology. To a certain extent, the international relation of space combat will evolve only *subsequent* to State action making such combat an imminent possibility. Because the law governs actual social relations and not theoretical abstractions, and because there have been no reported or anticipated cases of actual space combat, conclusions about legal restrictions on such combat must begin tentatively . . . . States faced a similar dilemma in the days leading up to World War I with aerial combat. At that time, one could hardly establish firm legal principles in the absence of State practice. As was the case in the 1910s with respect to air warfare, a great deal of original reflection on the implications of space combat is needed today.

Robert A. Ramey, *Armed Conflict on the Final Frontier*, 48 A.F. L. REV. 1, 3–4 (2000).

consequences of a cybersecurity attack, the United States must prepare to respond to the possibility.

As Richard A. Clarke observed in *Against All Enemies*, his account of America's counterterrorism failures leading up to the September 11, 2001, attacks, "America, alas, seems only to respond well to disasters, to be undistracted by warnings. Our country seems unable to do all that must be done until there has been some awful calamity that validates the importance of the threat."[224] Over the past two years, the country has received ample warnings of the consequences of cyberattacks, but the Executive Branch's legal ability to defend against such threats remains uncertain. Enacting the Cybersecurity Act outlined in this article would be a significant step toward empowering the Executive Branch to prevent such a calamity.

[224] CLARKE, *supra* note 222. The United States' experience in the aftermath of September 11, when Congress, in a six-week period, enacted a variety of previously unaddressed anti-terrorism legislation as the USA PATRIOT Act, suggests that rapid passage of Senator Rockefeller's proposal would be a likely product of a cybersecurity disaster. *See* Michael T. McCarthy, *Recent Developments: USA PATRIOT Act*, 39 HARV. J. ON LEGIS. 435, 437–39 (2002). This scenario bolsters this article's argument that Congress should enact a version of the Cybersecurity Act that improves on the deficiencies in Senator Rockefeller's bill.