Building Cyber Walls: Executive Emergency Powers in Cyberspace

Laura B. West*

Introduction

The Executive is granted broad authorities upon declaring a national emergency. As of this writing, there are thirty-five active declared national emergencies in the United States, the oldest of which dates back to the Iran Hostage Crisis in 1979.[1] Not surprisingly many of these continuing states of emergency—that last on average nearly ten years—address some facet of the war against terror.[2] These emergencies appear to illustrate that the American public acquiesced to broad grants of authority to the Executive; Americans seemingly yielded to the idea of a forever emergency, especially when it comes to terrorism. Recent declared emergencies, however, should heighten concerns about the appropriateness of such acquiescence for a forever emergency and invoke doubts about the permissible scope of the Executive's authorities.

The southern border wall emergency is a prime example. Declared by President Trump in February 2019, the border wall emergency quickly put the emergency powers under a microscope and subject to harsh public criticism.[3] Yet lurking under the radar of the border wall media frenzy is a nascent "endless emergency"[4] that arguably requires even more urgent attention—the cyberspace emergency.

---

* Major Laura West is a Judge Advocate in the U.S. Army and currently serves as the Deputy Chief of National Security Law at U.S. Cyber Command. Major West earned an LL.M., with distinction, from Georgetown University Law Center in National Security Law, an LL.M. from The Judge Advocate General's Legal Center and School in Military Law, a J.D. from William and Mary Law School, and a B.S. from the United States Military Academy. The views expressed in this article are those of the author and do not necessarily represent the views of the Department of Defense or any other government agency. I would like to thank Professors Mitt Regan, Mary DeRosa, and Carrie Cordero their thoughts that helped shape this article. I also wish to thank my husband, Brandon, for all of his expert advice and unwavering support. All errors are my own.

1. *See* Brennan Ctr. for Just., A Guide to Emergency Powers and Their Use (2019). President Trump declared an additional national emergency concerning the novel coronavirus on March 13, 2020, issued as this article went into editing. *See* Proclamation No. 9994, 85 Fed. Reg. 15,337 (Mar. 18, 2020).

2. *See id.*

3. *See, e.g.*, Peter Baker, *Trump Declares a National Emergency, and Provokes a Constitutional Clash,* N.Y. Times (Feb. 15, 2019), https://perma.cc/7S5D-3KST. Democratic leaders, Speaker Pelosi and Senator Schumer, described the emergency declaration as "plainly a power grab by a disappointed president, who has gone outside the bounds of the law to try to get what he failed to achieve in the constitutional legislative process." *Id.* The emergency declaration enables the President to divert $3.6 billion from military construction projects to the wall, if it withstands judicial scrutiny. *Id.* Congress had explicitly denied the construction of a wall and voted to the end the emergency, but the President vetoed the resolution, thus keeping the emergency in place. *See* Brennan Ctr. for Just., *supra* note 1.

4. *See* Jordan A. Brunner, Comment, *The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergency*, 57 Jurimetrics J. 397, 397-98 (2017).

In 2015, the first cyberspace emergency was declared by President Obama in response to the unique and then unprecedented 2014 Sony Pictures cyber hack by North Korea.[5] President Obama declared this national emergency to deal with the "unusual and extraordinary threat" of "malicious cyber-enabled activities."[6] The President continuously renewed this emergency since its inception.[7] In 2019, President Trump added another cyberspace emergency to the growing list of active emergencies. Pursuant to the Executive's emergency powers, President Trump declared certain telecommunications equipment, classified as a national security risk, to be banned from use by American companies.[8]

The advent of the cyberspace emergency requires careful and urgent attention for a number of reasons, the most pressing presented here. First, these emergencies come in the wake of an alarming rise in internet shutdowns around the world.[9] Internet shutdowns, touted by states as emergency methods for repelling massive cyber-attacks, are also documented as primary tools used by totalitarian regimes to stifle speech and dissent.[10] Second, running parallel to this growing internet shutdown movement, is the undeniable fact that the internet and telecommunications infrastructure are now an indispensable part of the nation's interconnected modern life, and is being threatened daily by ever-changing and growing malicious cyber-attacks. Finally, over the last year, a worldwide pandemic broke out and continues to take an unimaginable toll on Americans' daily existence and

5. The Sony Pictures hack was exceptional at the time; it was the first highly publicized attack that occurred in U.S. territory, covered in mainstream American media, and elicited a timely public government response. *See* CATHERINE A. THEOHARY, CONG. RESEARCH SERV., RL45142, INFORMATION WARFARE: ISSUES FOR CONGRESS, 7 (2018), https://perma.cc/WH9K-58YT (noting the unique nature of the Sony attack, to include "threats of physical destruction, affect[ing] the decision-making process of a private company, exploited the human element of fear in a civilian population, imposed extra-territorial censorship, and triggered a response from the U.S. government"); *see generally* Ellen Nakashima, *Why the Sony hack drew an unprecedented U.S. response against North Korea*, WASH. POST, (Jan.POST (Jan. 15, 2015), https://perma.cc/LML2-WZZC.

6. *See* Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015). Since the Sony hack, the U.S. imposed additional sanctions under cyberspace emergency authorities in 2016 and 2018 on Russia in response to cyber election interference. *See* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016); Exec. Order No. 13,849, 83 Fed. Reg. 48,195 (Sept. 20, 2018). In 2017, legislation was also implemented imposing further sanctions on Russia, Iran and North Korea due to cyber-related attacks. *See* Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44 (2017).

To note, this article uses the terms "cyber hack," "malicious cyber-enabled activities," and "cyber-attack" to mean in a general sense any type of malicious cyber operation. The term cyber-attack is used in this article as a colloquial term to better understand the scale and consequences of such an operation; however, it is not necessarily meant to be interpreted narrowly in the terms of an attack qualifying under the law of armed conflict. Such an analysis exceeds the scope of this article that is geared toward a domestic analysis. Specifically, this article is more focused on examining a "cyber-attack" as an operation that could encompass a wide range of incidents effecting cyberspace within the United States—it makes no reference to the intent or origins of the operations or attacks.

7. Continuation of the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, 84 Fed. Reg. 11,877 (Mar. 28, 2019).

8. *See* Exec. Order No. 13,873, 84 Fed. Reg. 37,055 (May 15, 2019).

9. *See* discussion *infra* Section II.A.

10. *See* Samuel Woodhams, *Contesting the Legality of Internet Shutdowns*, JUST SECURITY (Oct. 1, 2019), https://perma.cc/5ERS-DBM4.

human life. The nation's response to controlling the virus exposed critical vulnerabilities in national authorities and, unfortunately, demonstrates all too clearly how high the stakes are in refining national emergency authorities.

This state of affairs today raises the broad question of whether the United States government has appropriately tailored authorities and corresponding tools necessary to effectively defend against, recover, and maintain resilient networks during and after a massive cyber-attack. As mentioned above, the United States most notably responded to that question with a declared cyberspace emergency, unlocking significant broad authorities at the President's disposal to assist in the deterrence of such attacks.

But what is the true scope of a cyber national emergency authority? Imposing sanctions as President Obama did in 2015 with the first cyberspace emergency is likely only the tip of the iceberg for the scope of the Executive's emergency powers. More concerning and the focus of this article, though, is that similar to those totalitarian regimes, cyber national emergency powers may have a vast scope that goes so far as to permit the President to direct an internet shutdown, otherwise known as directing the proverbial "kill switch."

Most scholars who have tackled the internet "kill switch" subject come to a rather hasty conclusion that the President has the authority to shut down the internet under his emergency powers by invoking section 706 of the Communications Act of 1934 (codified as 47 U.S.C. § 606).[11] Over the years, this supposition has been debated on the fringes. This article adds to that debate, brings it front and center, and argues that the current legal authorities are wholly inadequate to address the possible need to quarantine, isolate, or shutdown computers or portions of the internet or networks within the United States in a time of emergency caused by a massive cyber-attack. Even if current domestic authorities can withstand the policy and legal scrutiny, the uncertainty and potency surrounding such authorities is enough to warrant new legislation that can provide "clear guidance and an enhanced ability to rapidly execute national level decisions for response options to sophisticated attack."[12] Accordingly, the time is now to rethink executive cyberspace emergency powers before there is a true need to build cyber walls.

Part II of this article illustrates the current cyber threat picture facing the United States. Part III then discusses the main target of these threats in cyberspace: the

11. *See* William Toronto, *Fake News and Kill Switches: The U.S. Government's Fight to Respond to and Prevent Fake News*, 79 A.F. L. REV. 167, 180 (2018); Jessica "Zhanna" Malekos Smith, *Where the Cyber Things Are*, 5 HOMELAND & NAT'L SECURITY L. REV. 1, 15-18 (2016); Scott Ruggiero, Comment, *Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch* 15 SMU SCI. & TECH. L. REV. 241, 241-42 (2012); Karson K. Thompson, *Not Like an Egyptian: Cybersecurity and the Internet Kill Switch Debate,* 9 TEX. L. REV. 465, 477 (2011); Gene Healy, *Emergency Exit Strategy*, CATO INST. (June 24, 2019), https://perma.cc/DGT6-DSEP; Elizabeth Goitein, *The Alarming Scope of the President's Emergency Powers*, THE ATLANTIC (Jan./Feb. 2019), https://perma.cc/YD8E-WY2G. *But see* David W. Opderbeck, *Does the Communications Act of 1934 Contain a Hidden Internet Kill Switch?,* 65 FED. COMM. L.J. 1, 17 (2013); *cf.* Paul Rosenzweig, *The Powers of Trump and the Internet "Kill Switch"*, LAWFARE BLOG (June 2, 2016), https://perma.cc/53PM-M5PT.

12. National Security Telecommunications Advisory Committee, *NSTAC Response to the Sixty-Day Cyber Study Group* Mar.(Mar. 12, 2009) [hereinafter *NSTAC*], https://perma.cc/99EP-KHZE.

internet. As a result, there arises the need to protect this target and potentially exercise the internet "kill switch" or an internet shutdown. Relatedly, part III of the article also provides a basic overview of the technology involved in an internet shutdown to address whether it is even possible to accomplish a shutdown in the United States. This background sets up for an analysis of the legal authorities that are potentially unlocked for the President to exercise during a declared cyberspace emergency, which is addressed in part IV. This section of the article grapples with whether those authorities can withstand scrutiny in light of the domestic legal framework, and ultimately shows that the President currently lacks the clear and assured power to unilaterally force a shutdown of the internet in the United States.

Nevertheless, the absence of a clear legal mechanism to exercise a type of shutdown during a cyberspace emergency may force the President to claim the use of these powers, almost certainly degrading any type of effective response. Thus, this article argues for Congress to provide new legislation that closes this gap. Part V proposes three options to reach this end state of filling the legal authority gap: a modified centralized shutdown authority, decentralized authorities with increased sector specific defenses, or a national cyber quarantine program. This article primarily advocates for the third option, or what is being offered as essentially a holistic national quarantine authority and supplemental program aimed at maintaining national "cyber health."

I. THE THREAT PICTURE

Identifying and understanding the cyber threat picture facing the United States is essential for further analysis of the legal authorities available to the government during a cyberspace emergency. Multiple aspects of the overall threat picture bear on the scope of the Executive's emergency powers. These aspects inform whether the United States needs internet shutdown authorities in the first place. To conduct this threat analysis, it is important to discuss what a massive cyber-attack might entail, both on a conventional and abstract level, including an evaluation of the potential targets of such an attack. Only then can the potential consequences from an attack be fully understood and inform the appropriate emergency response by the government.

A. Massive Cyber-Attack

Over the last decade, the United States has come to recognize cyber-attacks as one of the most significant emergent threats to national security.[13] The nature and scope of malicious cyber operations continue to evolve and grow. The world first took note of the devastating effects from a nationwide cyber-attack in 2007 that

13. *See, e.g.*, Dean DeChiaro, *At Ground Zero, Homeland Chiefs Say Cyber is a Top Future Threat*, ROLL CALL (Sept. 10, 2019), https://perma.cc/UN4S-XH2S. *Compare* Statement for the Record of Dan R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Jan. 29, 2019), https://perma.cc/LRU4-7R2X, *with* WHITE HOUSE CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (May 29, 2009) [hereinafter WHITE HOUSE CYBERSPACE POLICY REVIEW], https://perma.cc/5BN8-EVMM.

targeted Estonia's private and government networks.[14] In hindsight, though, the Estonia attack is now viewed as mild or simplistic in comparison to the attacks of today.[15] Ten years after the attack on Estonia, and only six months after the United States published a major piece of its national cyber response plan framework,[16] the world witnessed a "massive, coordinated cyber invasion" in 2017, the likes of which had not been seen before.[17]

According to reports, the 2017 massive cyber-attack involved Russia targeting Ukraine with the release of the NotPetya malicious code.[18] Russia's malicious cyber operations destroyed over 10% of computers in Ukraine.[19] Additionally, the destructive code "spread automatically, rapidly, and indiscriminately" beyond Ukraine's borders and into networks of governments, hospitals, global shipping companies, international firms, and banking companies, affecting at least 130 countries including the United States.[20] The cost of the NotPetya attack is estimated to be about $10 billion worldwide, surpassing the costs of the WannaCry attack that occurred only a month prior with costs ranging between $4 - $8 billion and an estimated reach of 100 countries.[21]

The far-reaching and devastating effects of the NotPetya and WannaCry malicious cyber operations are cause for concern and reason alone for the United States to reassess the effectiveness of the current U.S. emergency response authorities. Such attacks are unlikely to be the last or worst of its kind. Yet, even more concerning are the reports indicating that the hacking tools used in these attacks most likely came in part from stolen and leaked code developed by the National Security Agency.[22] This illuminates the very real threat that future attacks may not just be from adversary states, but rather could be generated from the unintentional release or theft of American cyber tools used on the nation's own networks.

B. Executive Use of Emergency Powers

With these conventional international and domestic threats in mind, it is important to consider a third and more abstract threat: the potential for government

14. *See* Toomas Hendrik Ilves, *Foreword* to TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, xxiii (Michael N. Schmitt ed., 2d ed. 2017).

15. *Id.*

16. *See* discussion *infra* Section V.A.

17. Andy Greenburg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED (Aug. 22, 2018), https://perma.cc/8LPM-E4W4.

18. *See id.*

19. *Id.*

20. *Id.*

21. *See id.*; Lily Hay Newman, *How an Accidental 'Kill Switch' Slowed Friday's Massive Ransomware Attack*, WIRED (May 13, 2017), https://perma.cc/E7QY-92XM.

22. *See* Greenburg, *supra* note 17; *see also* Bruce Schneier, *Why the NSA Makes Us More Vulnerable to Cyberattacks, The Lessons of WannaCry,* FOREIGN AFF. (May 30, 2017), https://perma.cc/J5EP-SLP4.

abuse or expansion of emergency powers generally.[23] The Trump administration held a very broad understanding of presidential emergency powers. While it may still be too early to determine whether the current Biden administration will continue an expansive use of emergency powers, a long line of such actions have been taken by presidents of both parties. Two very recent examples bear out this assertion.

First, as mentioned in Part I, President Trump's declaration of an emergency on the southern border with Mexico to build a wall creates concerns about presidential overreach with regard to emergency powers. In that case, President Trump asserted a state of emergency in order to unlock authorities that might allow the redistribution of previously appropriated funds not originally available for constructing a border wall.[24] President Trump faced challenges to the underlying emergency itself,[25] as well as a constitutional challenge alleging a violation of the separation of powers.[26] Specifically, the constitutional challenge asserts that the Executive encroached upon Congress' exclusive power of the purse under Article I of the Constitution,[27] in that, money cannot be reprogramed by the Executive when Congress previously denied its use.[28]

Still, if the Trump administration's border wall situation fails to cause concern, a second current example serves as a similar warning of potential future presidential overreach. In June 2019, a pro-democracy movement in Hong Kong spurred a large-scale disinformation campaign and the threat of internet shutdowns by the Chinese government.[29] In response to the unrest, in August 2019, President

---

23. *See* Goitein, *supra* note 11. Elizabeth Goitein clearly frames the issue of possible presidential overreach:

> In the past several decades, Congress has provided what the Constitution did not: emergency powers that have the potential for creating emergencies rather than ending them. Presidents have built on these powers with their own secret directives. What has prevented the wholesale abuse of these authorities until now is a baseline commitment to liberal democracy on the part of past presidents. Under a president who doesn't share that commitment, what might we see?

24. *See* Remarks by President Trump on the National Security and Humanitarian Crisis on our Southern Border (Feb. 15, 2019), https://perma.cc/5SE7-FS7F.

25. *See* Goitein, *supra* note 11. After declaring the emergency on the border, President Trump stated, "I could do the wall over a longer period of time. I didn't need to do this. But I'd rather do it much faster." President Donald Trump, Remarks by President Trump on the National Security and Humanitarian Crisis on our Southern Border, *supra* note 24. President Trump's own comments give light to the argument of unconstitutional overreach of emergency powers. *See, e.g.*, Quint Forgey, *'I didn't need to do this': Dems pounce on Trump's national emergency admission*, POLITICO (Feb. 16, 2019), https://perma.cc/3LRW-WGLW.

26. *See* Motion of Appellees' Answering Brief at 19-20, *Sierra Club v. Donald J. Trump*, Case No. 19-16336 (9th Cir. Aug. 15, 2019); Unopposed Motion for Leave to File and Brief of the U.S. House of Representatives as Amicus Curiae Supporting Respondents, at 1-2, *Donald J. Trump v. Sierra Club* (2019) (No. 19A60); *see also* Adam Liptak, *Supreme Court Lets Trump Proceed on Border Wall,* N.Y. Times (July 26, 2019), https://perma.cc/Q6UV-FA7B.

27. *See* U.S. CONST. art. I, § 9, cl. 7.

28. *See* sources cited *supra* note 26.

29. *See* Rachel Brown and Preston Lim, *U.S. Social Media Companies Block Accounts From China Over Hong Kong Disinformation*, LAWFARE (Aug.BLOG (Aug. 29, 2019), https://perma.cc/GFW7-YVTW.

Trump ordered American companies—via twitter—to start looking for alternatives to doing business with China.[30] After receiving criticism in the press about the order, President Trump followed up with a tweet stating that the International Emergency Economic Powers Act of 1977 (IEEPA) could give him such authority.[31]

This is not necessarily a partisan issue though, particularly given the long line of emergencies declared by presidents of both parties.[32] In both of these examples, the Executive cites to IEEPA as the source of broad Executive emergency authorities.[33] The issue then may be more aptly framed as the broad scope of IEEPA and how it is exercised by any particular administration.[34]

IEEPA generally allows for the Executive to declare a national emergency to deal with "unusual or extraordinary threats."[35] The Executive essentially has the power pursuant to IEEPA to freeze (or seize) any asset that might have bearing on what he determines to be such a threat, which is not clearly defined within the statute and comes with no explicit limits.[36] On its face, IEEPA could allow extremely broad powers because, for example, there is nothing that deters the Executive from determining that an American person is contributing to a foreign threat by affecting a foreign economy "through any transaction in foreign exchange."[37] Thus, it might be used to freeze out certain U.S. persons or entities that are providing some "material benefit" to a foreign threat or economy.[38] If IEEPA is interpreted this broadly, the result is then essentially what President Trump was insinuating when tweeting that IEEPA was a source of authority for the Executive to order U.S. companies to cease doing business with China.[39]

---

30. *See* Adam Edelman, *Trump Increases Tariffs on Chinese Goods Hours After Slamming Fed Chief*, NBC NEWS (Aug. 23, 2019, 9:21 AM), https://perma.cc/5QRE-BG3H.

31. *Id.*

32. *See* Rosenzweig, *supra* note 11; Goitein, *supra* note 11 ("What would the Founders think of these and other emergency powers on the books today, in the hands of a president like Donald Trump?").

33. *See* Scott R. Anderson & Kathleen Claussen, *The Legal Authority Behind Trump's New Tariffs on Mexico*, LAWFARE BLOG (June 3, 2019), https://perma.cc/X3ND-MD6V; Edelman, *supra* note 30 and accompanying text.

34. *See, e.g.*, Healy, *supra* note 11; *see also* BRENNAN CTR. FOR JUST., *supra* note 1 (discussing the level of reliance on IEEPA raises the concern that the actions being taken are not emergency actions at all, but the implementation of standard policy). "The International Emergency Economic Powers Act (IEEPA) allows the government to freeze any asset or block any financial transaction in which a foreign national has an interest, even if the asset belongs to an American or the transaction is between Americans." *Id.* Further discussion on IEEPA, as it relates to an internet shutdown, is discussed in Part V below.

35. International Emergency Economic Powers Act, 50 U.S.C. § 1701-1708 (2019) ("IEEPA").

36. *See* Brunner, *supra* note 4, at 407-08; *see generally* CHRISTOPHER A. CASEY, IAN F. FERGUSSON, DIANNE E. RENNACK & JENNIFER K. ELSEA, CONG. RESEARCH SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE, 10-26 (JULY 14, 2020), https://perma.cc/2KCH-VC4V (discussing scope and expanding use of IEEPA by the Executive over the years).

37. IEEPA, 50 U.S.C. § 1702(a)(1)(A)(i). The only deterrent to broad Executive interpretations of the statute might be obtaining a supermajority in Congress. *See* BRENNAN CTR. FOR JUST., *supra* note 1.

38. *See* Goitein, *supra* note 11; IEEPA, 50 U.S.C. § 1702(a)(1)(B).

39. To note, President Trump's "order" was never effectuated; it is extremely unclear what type of authority the Executive has to direct something of this magnitude via tweet and, in order to unlock

The reliance on and use of IEEPA for such broad authorities by any administration is, therefore, a threat to American values and civil liberties. Elizabeth Goitein, Director of Liberty and National Security at the Brennan Center for Justice, best summarizes this type of threat by stating, "[t]his level of reliance on an emergency power raises a different concern: that the actions being taken are not emergency actions at all, but the implementation of standard policy that should be bound by non-emergency law."[40] In sum, it is not just the use of these broad powers or authorities by the Executive that poses a significant risk, it is also the ability of the Executive to use these authorities during non-emergent situations to circumvent standing rule of law.

II. THE TARGET: TECHNOLOGY AND THE INTERNET

In light of the threats laid out above, it is important to determine whether an internet shutdown or a "kill switch" authority is even an appropriate mechanism to counter such threats in the United States. In other words, what can broad cyberspace emergency authorities really accomplish? What is even feasible for the government to do in cyberspace given the complex nature of U.S. internet technology and infrastructure? Answers to these questions help understand the current emergency authorities and provide direction for new proposals.

A. Internet Shutdowns

Civil rights advocacy groups sounded alarms over the significant rise in internet shutdowns worldwide.[41] Internet shutdowns have become the primary result of the use of cyberspace emergency authorities in other countries. One group recorded seventy-five government-imposed internet shutdowns worldwide in 2016 and 196 shutdowns in 2018.[42] Rising numbers show that this tactic does not seem to be going away any time soon, despite the overwhelming costs on a country implementing internet shutdowns.[43] The top official justifications for shutdowns are public safety and national security, while actual reasons may differ and range from political instability, protests, or violence.[44] Advocacy groups

IEEPA's broad authorities, the Executive would also have to declare an emergency. Moreover, the administration rolled back its stance a few days later after the G7 meeting in France. *See* Shannon Van Sant, *Trump Walks Back Statements On China; White House Walks Them Forward*, NAT'L PUB. RADIO (Aug. 25, 2019), https://perma.cc/2DNC-3GWM.

40. *See* BRENNAN CTR. FOR JUST., *supra* note 1.

41. *See, e.g.*, Woodhams, *supra* note 10.

42. Berhan Taye & Sage Cheng, *The State of Internet Shutdowns*, ACCESSNOW (July 8, 2019), https://perma.cc/SSC8-EJ7D.

43. *See generally* Darrell M. West, *Internet Shutdowns Cost Countries $2.4 Billion Last Year*, BROOKINGS INST. (Oct. 2016), https://perma.cc/3ZM9-FSFK; Woodhams, *supra* note 10. *But cf.* Greenburg, supra note 17 and accompanying text (the cost of a single cyber-attack cost approximately $10 billion).

44. *See* Taye & Cheng, *supra* note 42; *see, e.g.*, Mohammad Ali Kadivar, *Iran Shut Down the Internet to Stop Protests. But for How Long?*, WASH. POST (Nov. 27, 2019), https://perma.cc/D3JZ-A4SP (Iran shut down the internet in the face of violent protests against the government, claiming it was to maintain public order and security); Jeffrey Gettleman, Vindu Goel & Maria Abi-Habib, *India Adopts the Tactic of Authoritarians: Shutting Down the Internet,* N.Y. TIMES (Dec. 17, 2019), https://perma.cc/

generally claim that these disparate reasons for shutdowns are merely a smokescreen for violating human rights and civil liberties.[45] One group asserts, "shutdowns are always a violation and disproportionate means of protecting national security."[46]

To be sure, no Western countries are currently recorded as engaging in the practice. The majority of nations engaging in internet shutdowns come from Asia or Africa and typically struggle with political turmoil, human rights violations, and totalitarian regimes.[47] Russia recently added itself to this list of countries. The Russian government aggressively pursued internet shutdown authorities in its parliament for the stated purpose of protecting against cyberwar.[48] Russia announced plans to disconnect from the global internet as early as April 2019 to conduct tests of their internal intranet "RuNet" that is expected to operate during times of national emergency.[49] The "Sovereign Internet" bill became law in 2019 and allows the Russian government to cut off the country's internet traffic from foreign servers in the name of security threats.[50]

The cast of countries engaged in the practice of shutdowns and the implications on human rights and civil liberties certainly paints a bleak picture for establishing or implementing similar authorities in the United States. However, this is not the end of the story. Cyberspace emergency authorities are not limited to unstable, totalitarian, or adversarial states.[51] India, the world's largest democracy, shuts down the internet more than any other country.[52] Additionally, many partner nations of the United States have modern laws on the books, albeit in most cases dormant, that would explicitly allow for an internet shut down. In the United Kingdom, for example, an internet shutdown authority is part of the Communications Act of 2003.[53] Although the authority has yet to be exercised, it remains an available and transparent option during a national emergency to protect the public and safeguard national security.[54] The emergency provision in the U.K. Communications Act, in conjunction with the 2004 U.K. Civil Contingencies Act, are tailored authorities that

9K84-QZKN (India increasingly uses internet shut downs for everything from security to stifle exam cheating).

45. *See* Woodhams, *supra* note 10.

46. *Id.*

47. *See* Taye & Cheng, *supra* note 42.

48. See Zak Doffman, RUSSIAN AUTHORITIES 'SECRETLY' SHUT DOWN MOSCOW'S MOBILE INTERNET: REPORT, FORBES (Aug. 8, 2019), https://perma.cc/M4NN-YCN5.

49. *See, e.g.*, Tamara Evdokimova, *Will Russia Disconnect From the Internet on April 1?*, SLATE (Mar. 29, 2019), https://perma.cc/MVX6-68WV.

50. *See* Jan Lindenau, *Russia's Sovereign Internet Law Comes Into Force*, THE MOSCOW TIMES (Nov. 1, 2019), https://perma.cc/JU9B-FURH; *Russia: New Law Expands Government Control Online*, HUMAN RIGHTS WATCH (Oct. 31, 2019), https://perma.cc/QYZ5-9K5T.

51. Turkey, a NATO partner, has engaged in internet shutdowns as well. As of 2018, one government-imposed shutdown was recorded in Turkey. *See* Taye & Cheng, *supra* note 42.

52. Gettleman et al., *supra* note 44.

53. *See* Communications Act, 2003, c. 21 § 132 (Eng.).

54. *See* Nick Harding, *Could the UK Government Shut Down the Web?*, INDEPENDENT (Mar. 8, 2011), https://perma.cc/VG4M-DYPJ. The U.K. Communications Act works in conjunction with the 2004 Civil Contingencies Act to give the authority to suspend internet services. *Id.*

provide safeguards, such as, general limits on the authority, statutory avenues for recourse if the powers are abused, and a thirty day time limit on stated emergencies.[55] Such cyberspace emergency authorities, therefore, appear to be a legal option that any government—democratic or otherwise—may want available to use in case of a cyberspace emergency.

It should come as no surprise then that President Trump advocated for shutting down portions of the internet to combat terrorism in both 2015 and 2017.[56] Yet, the question remains: even if the United States had a similar appropriately tailored shutdown emergency authority as the United Kingdom, would it effectively prove worthless based on the complex nature of the internet in the United States? This question requires a brief—albeit simplified—summary of the internet structure in the United States and how a shutdown authority might operate in practice.

B. The Technology

Many scholars already wrestled with the question of whether a shutdown authority can be accommodated by the U.S. internet structure.[57] Some addressed the issue in the context of an internet "kill switch," taking the very literal meaning of a singular switch to shut down the entire internet.[58] A switch of this nature is most certainly a thing of fantasy, notwithstanding speculation about the unknown scope or reach of a secret government program.[59]

Instead, the internet kill switch should be thought of in a different and very real way. When the debate regarding an internet kill switch was at its apex in 2012, Paul Rosenzweig rephrased the "kill switch" issue rather succinctly by stating, "[w]hat (if any) powers should the President have to direct private sector actors to take action (to and including shutting down access to portions of the network) in a time of emergency?"[60] In other words, although "kill switch" has been the colloquial term used in debates, based on the complex nature of the internet and networks in the United States, the "kill switch" is really a concept that should be

55. *See id.*; Communications Act § 132.

56. Sam Frizell, *Donald Trump Wants to Close Off Parts of the Internet*, TIME (Dec. 6, 2015), https://perma.cc/33PV-4CMR; Chris Matyszczyk, *Trump Calls for Internet to be Cut Off for Terrorists*, CNET (Sept. 15, 2017, 8:52 AM), https://perma.cc/U94G-SSCQ; David Goldman, *Donald Trump Wants to 'Close Up' the Internet*, CNN (Dec. 8, 2015), https://perma.cc/E44N-GV2Y. Although these examples are more appropriately categorized as offensive cyberspace activities in support of combat operations abroad that can be distinguished from domestic internet shutdowns directed under emergency authorities, the example shows that the idea of internet shutdowns remains on the shelf as an option to address national security concerns. In both cases, President Trump actually called on U.S. internet ISPs and infrastructure providers to effectuate such a shutdown. *See id.*

57. *See* sources cited *supra* note 11. Some assert that shutting down the internet, or at least some portions, would be an impossible task in the United States. *See, e.g.*, Goldman, *supra* note 56.

58. *See, e.g.*, Alyssa Newcomb, *SXSW 2017: Is There Such a Thing as an Internet Kill Switch?*, NBC NEWS (Mar. 10, 2017), https://perma.cc/9PCP-4RT6.

59. *See* Toronto, *supra* note 11, at 183-85.

60. Paul Rosenzweig, *The Internet "Kill Switch" Debate,* LAWFARE (Feb.BLOG (Feb. 2, 2012), https://perma.cc/XUP8-98JP. This paper adopts this understanding of the "kill switch" concept and attempts to answer that question.

understood to mean: legal or statutory authority for the Executive to direct the shutdown of networks or portions of the internet in a time of emergency.

As a starting point, there is clear evidence that internet shutdowns occur on a global scale cutting off access to the "world wide web," a structure intended to connect the world through a series of decentralized interconnected networks and connection points where if one route goes down then information is merely sent through another route to get to its destination.[61] It is a system designed for redundancy and constant availability.[62] Despite this structure that was built to keep information flowing, look no further than to the various shutdowns across Asia and Africa for evidence that there are ways to stop that information flow. The specific anatomy of shutdowns worldwide has ranged from bandwidth throttling, broadband and mobile internet shutdowns, internet blanket blackouts, telecommunications blackouts and service-specific (platform) shutdowns.[63] Shutdowns become an even more salient reality with increased efforts among states in the last few years like those in Russia to create more centralization, rather than decentralization, in their internet infrastructures for the sake of national security.[64]

The obvious counterargument to this is that the internet in countries engaging in shut downs, such as Egypt—for instance, in its seminal government-imposed shutdown in 2011—is relatively easy to shut down due to the limited number of access points for information flowing into the country.[65] In stark contrast, the internet (or cyberspace) structure serving most of the United States is far more complex, with greater amounts of networks and connection points mostly controlled by private entities, than a country like Egypt that has a relatively simple internet infrastructure.[66] Most assuredly this is a valid argument, but not dispositive.

In the United States there are currently over 2,500 internet service providers (ISPs), but only approximately a dozen major ISPs that handle a majority of internet traffic.[67] Americans connect to the internet in a variety of ways. As of

61. *See generally* Allan Friedman & P. W. Singer, Cybersecurity and Cyberwar: What Everyone Needs to Know 16-18 (Oxford Univ. Press 2014).

62. Robert Morgus & Justin Sherman, *The Idealized Internet vs. Internet Realities [Version 1.0]*, NEW AMERICA (July 26, 2018), https://perma.cc/2334-4WNT. But, "the internet's physical infrastructure is [also] filled with so-called "'choke points"points' where single companies or governments control massive flows of information—creating single points of failure (SPOFs) that challenge the principle of resilience." *Id.*

63. Taye & Cheng, *supra* note 42; *see* West, *supra* note 43, at 2; *see also* April Glaser, *It'd Be Crazy Easy for Brazil to Block the Web Right Now,* WIRED (Aug. 11, 2016), https://perma.cc/B7JX-DGWE (describing other methods of shutting down the internet or specific services, like modifying routing tables and working with the ISPs to block access).

64. *See* Morgus & Sherman, *supra* note 62.

65. *See* Jordan Robertson, *The day part of the Internet died: Egypt goes dark*, WASH. TIMES (Jan. 28, 2011), https://perma.cc/6P2S-BMTS.

66. *See id.*; *see also* Timothy B. Lee, *40 Maps That Explain the Internet*, VOX (June 2, 2014), https://perma.cc/VG2J-XAYP (compare maps 18, 17, 8, and 7, showing the complex nature of the United States internet backbone and a comparison to Egypt).

67. *See* Lee, *supra* note 66; *The Complete List of Internet Providers in the US*, BROADBAND NOW, https://perma.cc/C6HC-U6U8; cf. Ingrid Burrington, *Tracing the Byzantine Maze of the Companies*

December 2017, approximately 75% of Americans connected to the internet using mobile wireless services, with the rest connecting through some fixed method such as wirelines (e.g., Digital Subscriber Lines), satellite, or cable modems.[68] Internet users' data travels through a series of checkpoints, including local ISPs, long-haul providers, and network exchanges.[69] Major checkpoints moving data could potentially serve as a chokepoint,[70] but the scale at which those checkpoints would need to be shut down depends on the scale of the target, thus making the task in the United States seem insurmountable.

In practice, the United States government is highly unlikely to shut down the entire internet, especially considering virtual private networks (VPN) and mesh networks that would pop up in a shut down.[71] The more likely scenario, however, is a targeted quarantine, isolation, or shutdown of specific computers or networks. Viewing a shutdown on a more granular level begins to reveal its feasibility and utility to the government for public safety and national security reasons.[72]

There are plenty of prior examples of smaller scale quarantines or shutdowns of specific computers or networks in the United States. In the private sector, for instance, a university might regularly practice blocking computers from network access,[73] or critical infrastructure sectors may institute data quarantine programs through software design (e.g., using a software designed network) to thwart

---

That Have Come to Control America's Internet, QUARTZ (Oct. 5, 2016), https://perma.cc/PPT8-34YU (explaining that only a handful of ISPs have complete coverage over the United States and most ISPs are subsidiaries of the larger companies); Ramakrishnan Durairajan, Paul Barford, Joel Somers & Walter Willinger, *InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure*, 45 ACM SIGCOMM COMM. REV. (2015), https://perma.cc/Y6EU-HGBX (showing a digestible level of internet connections, nodes, links, or conduits in the United States made possible by mapping all of the U.S. long-haul fiber-optic infrastructure, and suggesting that the infrastructure actually poses a risk to U.S. connections due to its overall lack of diversity and identifiable chokepoints).

68. *See* Fed. Commc'ns Commission, Industry Analysis Division Off. of Econ. & Analytics, Internet Access Services: Status as of December 31, 2017, 12, 16 (2019), https://perma.cc/9LBG-NVY2.

69. *See The Structure of the Internet*, WEBFX (Mar. 25, 2020), https://perma.cc/SF4Y-NRUJ; *see also* Durairajan et al., *supra* note 67.

70. *See* Morgus & Sherman, *supra* note 62.

71. The often-used analogy of a road system is useful in visualizing this issue. If, for example, the government wanted to shut down Washington, D.C. from the rest of the world, it would need to shut down all the major highways, connecting roadways, rail stations, and airports. Shutting down the major highways alone may have a significant impact. Yet, despite all these efforts, people may still be able to get in by foot. In cyberspace, mesh and VPN networks might be thought of as those individuals getting in by foot. Mesh and VPN networks are frequently used by citizens in countries that utilize internet shutdowns. *See, e.g.*, James Griffiths, *Blocking Social Media Would be 'the End of the Open Internet of Hong Kong.' It Also Wouldn't Work,* CNN (Aug. 29, 2019), https://perma.cc/RH2D-XULD; *see also* Woodhams, *supra* note 10.

72. On the contrary, some might argue that taking a granular view of the internet is inapposite to how it operates generally, since if you shut down one "roadway" another one just opens up. But this might depend on how you target the "roadways" and what you aim to accomplish from a shutdown (e.g., requiring users to manually shut down their networks thus shutting it down at the end point, shutting down directed service through the ISP, shutting down data centers, or shutting down long-haul service providers).

73. *See, e.g.*, Office of Information Technology, *Network Block*, U. OF CALI., IRVINE, https://perma.cc/X6RR-KUXZ.

cyber-attacks.[74] There have also been cases of inadvertent network shutdowns in the United States,[75] showing the feasibility of a smaller scale shutdown.

The U.S. government has also engaged in similar practices in non-emergency situations. One such example was in 2012 when the Department of Justice (DoJ) requested and received a court authorization for the government to take over servers in the United States that were used to orchestrate a large campaign of spreading malicious code.[76] In addition to the court order, the DoJ and Federal Bureau of Investigation in that case (otherwise known as the "DSNchanger shutdown") relied on voluntary cooperation from ISPs to further cut off infected computers' access to the network.[77]

The government led "DSNchanger shutdown" illuminates the possible need for a shutdown authority in emergency situations. The shutdown shows how the U.S. government took steps to stop the spread of a computer virus by taking over malicious servers. The government, however, had to accomplish this over many months by working with ISPs to block individual users from networks on a voluntary basis and pursuant to court orders. Those court orders were heavily reliant on judicial interpretation of cyber threats and subjective timelines needed to address those threats.[78] So, while this shutdown serves as evidence that a government quarantine, isolation or shut down process has significant value and a place in the nation's cyber incident response tool-kit, it also highlights how long the process may take through court proceedings and raises questions about the efficacy of this process in an emergency situation.

Generally speaking, therefore, quarantine or shutdown authorities might be used to slow or stop the spread of malicious attacks or take vulnerable or targeted computers off networks, as was the case with the DSNchanger shutdown. Additionally, such authorities might be used to delay or disrupt attacks, issue anti-virus files or patches,[79] or merely conduct forensics on computers subjected to an attack. All of these incident response mechanisms might be desirable, if not

74. *See, e.g.*, Letter from U.S. Commc'ns Sector Coordinating Council to Nakia Grayson, National Institute of Standards and Technology, 8 (Sept. 15, 2016), https://perma.cc/HDQ6-A9KL (discussing the use of Software Designed Networks to quarantine data, shift resources, or limit an attacker's access to resources outside a specific data set, which helps limit the impact of an attack and speed recovery).

75. *See, e.g.*, Lily Hay Newman, *How a Tiny Error Shut Off the Internet for Parts of the US*, WIRED (Nov. 6, 2017), https://perma.cc/5RLA-RWP8.

76. *See* Brian Krebs, *Court: 4 More Months for DSNChanger-Infected PCs*, KREBS ON SECURITY (Mar. 6, 2012), https://perma.cc/Y7FC-G2FT; *see also* Hayley Tsukayama, *Hit with DNS Changer Shutdown? Here's What to Do.*, WASH. POST (July 9, 2012), https://perma.cc/CP8L-6VFF; *Up to 500, 000 Internet Users to Lose Access as FBI Blocks Computers Infected with Virus*, DAILY MAIL (UK) (July 8, 2012), https://perma.cc/9XE7-BYGD (showing the global reach of such incident response that even computers in the United Kingdom could be effected).

77. *See* Krebs, *supra* note 76.

78. *Id.*

79. For example, the NotPetya attacks required patches in vulnerable computers to stop its spread. *See* Greenburg, *supra* note 17; *Patch Remote Desktop Services on Legacy Versions of Windows*, NAT'L SEC. AGENCY (June 4, 2019), https://perma.cc/JD3Q-8FWM.

necessary, during an emergency situation that does not afford the time to obtain court orders or depend on private sector cooperation.

But this raises the core issue here, which is whether the Executive is really using such powers in a time of true emergency and thus whether Congress should give the Executive such broad powers in the first place. At the end of the day, there is a balancing act that has to be performed that involves balancing government powers, national security, and civil liberties. As such, it is important to analyze current authorities available to the Executive to see if they already strike the appropriate balance.

III. EXECUTIVE CYBERSPACE EMERGENCY POWERS LEGAL ANALYSIS

A. Constitutional Framework

Any analysis of the Executive's emergency powers must necessarily start with the seminal case of *Youngstown Sheet & Tube Co. v. Sawyer*.[80] During the Korea conflict, President Truman wanted to seize the steel mills during a strike.[81] The question in *Youngstown* was whether the President had the power to authorize the nationalization of the steel mills. Simply put, the Supreme Court said no, finding that Congress handles strikes as a labor relations issue and did not give that authority to the President.[82] The majority opinion authored by Justice Black reasoned that this power was more appropriately a congressional power given the enumerated powers in the Constitution.[83] The Court viewed any authority to seize property an inherent congressional authority that must be delegated to the President.[84] Justice Black summarized:

> The President's power, if any, to issue the order must stem either from an act of Congress or from the Constitution itself. There is no statute that expressly authorizes the President to take possession of property as he did here. Nor is there any act of Congress . . . from which such a power can be fairly implied.[85]

Youngstown established that there are no general emergency powers separate from statutory or constitutional authority; a statutory authority would be required to imply any power.

While the *Youngstown* majority opinion frames how to view sources of authorities, it is Justice Jackson's concurrence that offers a timeless and practical framework for analysis. Jackson provided three categories for analysis in his

80. *Youngstown Sheet & Tube Co. v. Sawyer,* 343 U.S. 579, 587 (1952) (holding that President Truman did not have the power to seize the steel mills, despite the existence of a declared emergency, and that the President's power must stem from an act of Congress or the Constitution).

81. *Id.* at 583.

82. *See id.* at 586.

83. *See id.* at 582, 587-89.

84. *See id.* It is important to note that Congress "deemed seizure so drastic a power as to require that it be carefully circumscribed whenever the President was vested with this extraordinary authority." *Id.* at 598 (Frankfurter, J., concurring).

85. *Youngstown*, 343 U.S. at 585.

concurrence. The first category establishes the circumstances when the Executive operates with maximum authority, which includes times when either the Executive is acting with inherent authority or, alternatively, with specific congressional authorization.[86] The second category establishes that the Executive operates in the "zone of twilight" when there is an absence of either a congressional grant or denial of authority.[87] Finally, the third category establishes the point at which the Executive acts at the "lowest ebb" of his authority.[88] This "lowest ebb" category entails presidential actions directly contrary to the intent of Congress or acts incompatible with the express or implied will of Congress.[89] A court could only sustain presidential action that fell into this category if the action was "within his domain and beyond control by Congress."[90]

In 1976, almost a quarter century after *Youngstown*, Congress passed the National Emergencies Act (NEA). Congress created NEA to restrain presidential emergency power that was thought to be too broad at the time. Before NEA was passed, "approximately 470 separate sections of the United States Code were found . . . to delegate to the President a vast range of powers embracing every aspect of American life."[91] Congress intended to reign in some of these vast powers with the Act by still allowing the Executive to have discretion in issuing an emergency declaration, but now requiring the Executive to specify which powers the Executive intends to use.[92] In short, pursuant to NEA the Executive needs to point to a separate authority to do whatever act the Executive claims he or she can do in an emergency. The Act essentially codified what was already part of the *Youngstown* precedent.[93]

Considering the above legal landscape, to conduct an analysis on the scope of the Executive's cyberspace emergency powers, it should be considered what separate authority the Executive has to order an internet shutdown and whether such a claim can withstand scrutiny after an analysis under Jackson's three categories. Prior to moving into this analysis, though, the stage must be set with a general appreciation of applicable constitutional authorities bestowed upon the Executive and Congress and the corresponding main counterarguments these authorities present.

---

86. *Id.* at 635-637 (Jackson, J., concurring).

87. *Id.* at 637.

88. *Id.* at 638.

89. *Id.*

90. *Youngstown*, 343 U.S. at 640 (Jackson, J., concurring).

91. Aaron S. Klieman, *Preparing for the Hour of Need: The National Emergencies Act*, 9 PRESIDENTIAL STUD. Q. 47, 54 (1979).

92. Goitein, *supra* note 11; *see* National Emergencies Act, 50 U.S.C. § 1621 (2019) [hereinafter NEA] ("With respect to acts of Congress authorizing the exercise, during the period of a national emergency, of any special or extraordinary power, the President is authorized to declare such national emergency.").

93. *But cf.* Goitein, *supra* note 11. Goitein posits that NEA has failed by any objective measure to accomplish its aim, despite the law providing ample procedural requirements on the President's exercise of emergency powers. *See id.*

The Constitution offers scant authority for the Executive to act generally, let alone any exclusive or concurrent authority in this area. It is Congress' exclusive authority to provide for the common defense and general welfare of the United States,[94] which a shutdown may properly fall under. Also, *Youngstown* discusses, any seizure of property or restraints on American interests are an inherent authority of Congress under its law-making authority that must be delegated to the President.[95]

On the contrary, an argument can certainly be made that a shutdown may be conducted pursuant to the Executive's exclusive powers to conduct foreign relations and serve as the Commander-in-Chief of the armed forces if faced with a foreign cyber threat.[96] However, both of these authorities fail to appreciate the full scope of an internet shutdown. The use of these authorities would direct the targets of military defensive or offensive measures at U.S. persons' property and rights. The targeting of U.S. persons and private sector infrastructure is outside the mission of the U.S. military, even if doing so is in support of civil authorities or the Department of Homeland Security since these entities also lack such authority outside of U.S. person or private entity consent. National security practitioners today identify this divide in Executive foreign and domestic authorities as a vulnerable seam in the legal framework that can be exploited by malicious cyber actors or adversaries.

Alternatively, one might also try to analogize a shutdown in cyberspace to a military blockade of ports as in the famous *Prize Cases*.[97] That again misses the mark. While the internet might make for an easy comparison to a transport system as in the *Prize Cases*, the internet today has become much more than a transport system for information, making the analogy unworkable in a real sense. It is also not the type of "enemy property" considered in the *Prize Cases*;[98] it is domestic U.S. persons' property at issue. But the internet is far more than property, it has become an integral part of modern life, making up a global "ecosystem," that impacts the fundamental rights of every American.[99]

To conclude this initial step, since the Constitution does not afford the President the authority to effectuate an internet shutdown, specific statutory authorities provided by Congress must be considered. The next part of this article takes a much closer look at this critical step in the analysis.

---

94. U.S. CONST. art. I, § 8, cl. 1.1.

95. *See supra* notes 82-84 and accompanying text.

96. U.S. CONST. art. II, § 2, cl. 1-2.

97. *See generally The Prize Cases*, 67 U.S. 635 (1863) (finding permissible Executive action when dealing with the capture of enemy ports by blockade).

98. *See Padilla v. Rumsfeld*, 352 F.3d 695, 717-18 (2d. Cir. 2003) (discussing how the *Prize Cases* were not adequate for comparison to cases that involved the capture of enemy property or involved the deprivation of U.S. citizen rights).

99. *See* West, *supra* note 43, at 1-2; s*ee* discussion *infra* Section IV.B.3.

B. Challenging the "Kill Switch" Statutory Authority

1. The "Kill Switch" Authority Background

After the 2007 cyber-attacks against Estonia, the U.S. government began exploring the impact of cyber incidents and pushing for improved cybersecurity policy and guidance.[100] There was a general recognition within government that "clear guidance" and "response options" were lacking to defend against massive cyber-attacks.[101] During this period, the Obama administration aggressively forged plans, conducted studies, and issued guidance to identify and address gaps in government cyber incident response efforts.[102] Many of these studies, however, revealed that both the government and the private sector were not prepared for a massive national cyber-attack.[103]

To address this threat, members of Congress proposed responsive legislation, such as the Protecting Cyberspace as a National Asset Act of 2010 (PCNAA). The PCNAA was the primary legislative effort in a series of bill proposals from 2010 through 2012 that attempted to establish a more comprehensive framework for incident response and cybersecurity oversight.[104] Significantly, this series of legislative attempts failed in Congress over the next few years due in part to controversial provisions regarding the Executive's authority to issue declarations of a national cyberspace emergency, which would allow for the Executive's effective control or shutdown of critical cyber infrastructure.[105] The legislative provisions

---

100. *See NSTAC*, *supra* note 12.

101. *Id.*

102. *See generally* The White House, Foreign Policy, *The Comprehensive National Cybersecurity Initiative*, https://perma.cc/9QSE-WFQC. For instance, the Department of Homeland Security modified its EINSTEIN cybersecurity system in 2008 to identify malicious or potentially harmful computer network activity in federal government networks; moving beyond its prior capabilities of merely recording network traffic. DEP'T OF HOMELAND SEC., EINSTEIN, https://perma.cc/S3WH-6EYX.

103. *See, e.g.*, WHITE HOUSE CYBERSPACE POLICY REVIEW, *supra* note 13 (advocating for the work that needed to be accomplished to change the entire Nation's cybersecurity approach that had "over the past 15 years . . . failed to keep pace with the threat").

104. *See generally* Protecting Cyberspace as a National Asset Act, S.3480, 111th Cong. (2010) [hereinafter PCNAA]. The PCNAA attempted to establish central entities to coordinate incident response among government and the private sector. *See id.* Between 2011-2012, two additional bills failed that attempted to address and alleviate concerns about the authority of the government to shut down the internet in times of emergency. For a detailed discussion of this legislative history, see Opderbeck, *supra* note 11, at 4-6 and David Opderbeck, *Cybersecurity and Executive Power*, 89 WASH. U. L. REV. 795, 801-11 (2012). After the failure of these bills, the legislative debate then shifted from controversial authorities to information disclosures and general cybersecurity compliance. Opderbeck, *supra* note 11 at 5.

105. *See* Opderbeck, *supra* note 11, at 3. To be sure, the legislation was also hotly debated due to its provisions that attempted to set up cybersecurity standards for the private and government sector. The private sector desired market forces to effect cybersecurity protections and reiterated the deep seeded position a light-touch government approach to regulation in cybersecurity so as to not disrupt innovation and a free market in the developing cyber area. *See, e.g.*, Letter from U.S. Chamber of Commerce, *Key Vote Letter on S. 3414, the "Cybersecurity Act of 2012",* to U.S. Senate (July 30, 2012), https://perma.cc/82SH-DXLQ. The kill switch provisions, however, received some of the most scrutiny and were most curtailed throughout the 2010 - 2012 revisions between bill proposals. *See, e.g.*, Greg Nojeim, *Does*

became known as the "kill switch" provisions.[106]

The "kill switch" provisions or shutdown authority in the PCNAA and in subsequent legislative proposals were hotly debated. In the PCNAA, the President would have the ability to declare a cyberspace emergency, unlocking the authority to have full control over internet networks and isolate critical infrastructure from any attack for up to thirty days with possible extensions up to 120 days with a joint resolution.[107] During the Senate Committee on Homeland Security and Government Affairs hearings, proponents of the bill advocated for the "kill switch" provisions claiming it was a restraint on the President's powers that might already be available to him under the Communications Act of 1934.[108] For comparison, it is worth noting that the proposed emergency powers in the PCNAA were only slightly broader than those contained in the U.K. Communications Act of 2003 discussed in Part III.A. above. The debate surrounding the "kill switch" provisions not only shows just how broad in scope the Communications Act of 1934 might be, but also how unsuccessful efforts in the past have been to curtail such broad authorities. Ironically, the legislative efforts from 2010 through 2012 to pass a "kill switch" authority failed due to fears of broad presidential powers, when in reality the legislation was proposed to curtail the existence of authorities that some thought give the President even broader powers.[109]

Despite the controversy surrounding this authority and the failure of the legislation, executive branch officials continued to hold the position that the President already has the authority to shut down the internet or portions of networks under section 706 of the Communications Act of 1934 (codified as 47 U.S.C. § 606) [hereinafter "section 606"].[110] Most scholars point to Senate committee testimony in 2010 surrounding the PCNAA as the basis for this supposition of presidential power.[111] This might suggest Congress' acceptance of the Communications Act as a source of "kill switch" authority for the President. Today, many scholars take this assertion at face value, suggesting that there is no more constitutional heavy lifting to be done here since Congress "has acted" in giving the President the authority to effectuate a shutdown.[112] In other words, the predominant argument is that under the *Youngstown* analysis, the President could act pursuant to the Communications Act to shut down the internet with "maximum legitimacy."[113]

Senate Cyber Bill Include an 'Internet Kill Switch"?, CDT (Feb. 23, 2011), https://perma.cc/489G-UUNL.

106. *See id.* at 807; Megan Carpentier, *Joe Lieberman And The Myth of The Internet Kill Switch*, TALKING POINTS MEMO (June 21, 2010), https://perma.cc/QNX5-DN2G.

107. *See* Protecting Cyberspace as a National Asset Act, S.3480, 111th Cong. § 249.

108. *See* Carpentier, *supra* note 106.

109. *See id.*

110. *See* S. REP. NO. 111-368 at 10 (2010).

111. *See id.*; *see also* Rosenzweig, *supra* note 60.

112. *See, e.g.*, sources cited *supra* note 11; *see also* Sean Lawson, *The Law That Could Allow Trump To Shut Down the US Internet*, FORBES (Dec. 2, 2016), https://perma.cc/W557-3ZK9.

113. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 587, 635 (1952) (Jackson, J., concurring).

However, it appears more likely that Congress' acknowledgement of "kill switch" authority was rather limited to the legislative debates by the bills' proponents at the time. There is no evidence of widespread acknowledgement by Congress for this authority. In fact, the first time the Communications Act appeared as a listed source of authority for the President in cyberspace was in the Obama Administration's 2009 Whitehouse Cyberspace Policy Review.[114] Further, it was Philip Reitinger, then Department of Homeland Security (DHS) Deputy Undersecretary, a member of the executive branch, that provided the initial testimony in Congress in 2010, asserting "Section 706 of the Communications Act and other laws already address Presidential emergency authorities and Congress and the Administration should work together to identify any needed adjustments to the Act, as opposed to developing overlapping legislation."[115]

Critically, the debate over section 606 of the Communications Act has never been fully resolved. While the debate around the "kill switch" authority remains dormant for now, it is still very much alive and a threat to security if it remains in its current state of uncertainty.[116] The analysis below argues that it is time to put the final nail in the coffin of this alleged presidential cyberspace emergency authority.

2. The Communications Act of 1934 is Not a "Kill Switch" Authority

Pursuant to 47 U.S.C. § 606(d) (Section 706 of the Communications Act), the President is granted war powers that enable him to "suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission," subject to temporal limitations.[117] Some scholars point to this war powers provision, section 606(d), referencing *wire* communications as a source of emergency internet shutdown authority.[118] To clarify, that contention is misplaced for the most part. Section 606(d), regarding *wire* communications, requires a "state or threat of war" rather than a mere declaration of an emergency to unlock its authority.[119] Thus, when analyzing emergency powers generally,

114. *See* WHITE HOUSE CYBERSPACE POLICY REVIEW, *supra* note 13, at n.8.

115. *See* S. Rep. No. 111-368 at 10 (2010).

116. Opderbeck, *supra* note 11, at 5.

117. 47 U.S.C. § 606(d).

118. *See* Goitein, *supra* note 11 (referencing wire communications). Congress has made distinctions between *wire* communications and *electronic* communications since the enactment of the Communications Act, despite these distinctions blurring over time. *Cf.* Electronic Communications Privacy Act, Title I, 18 U.S.C. §§ 2510 *et seq*. The internet, although composed of many wire connections throughout its infrastructure, more aptly falls under the electronic communications category that is outside the scope of the Communications Act, which is further emphasized by FCC interpretations discussed *infra*. Additionally, an analysis of the legislative intent and agency interpretations of the Communications Act should also influence interpretations of this war provision. For these reasons, this article focuses on the more specific emergency authorities proscribed for the Executive in section 606(c) of the Communications Act.

119. *See* 47 U.S.C. § 606(d).

section 606(c) serves as the more appropriate starting point since in most cases there may not be a state or threat of war. As history has shown, a cyber-attack in most cases will likely not rise to the level of a state or threat of war.

Section 606(c) permits the President to declare a state of emergency that would allow him, "if he deems it necessary in the interest of national security or defense, . . . [to] suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations."[120] Focusing on the emergency authority, the argument is that these provisions contain the "kill switch" authority because the law permits the President to take over any *device* that emits radiofrequency transmissions.[121] Today that could be interpreted to include every electronic device that has electricity running through it.[122] But, that was not entirely the case in 1934.[123]

This leads to the first—and most obvious—reason why the Communications Act of 1934 (the Act) does not contain a "kill switch" authority, which is that Congress passed the legislation in the radio era, multiple decades before the internet was even a rational thought.[124] Therefore, Congress could not have contemplated covering the internet under the Act. One could argue that this era gap is irrelevant because the provisions were intentionally drafted broad enough to cover any advancements in technology over time.[125] In fact, this is the primary counter argument espoused today. Nevertheless, a review of the legislative history, subsequent agency interpretations and legislation bears out otherwise, as addressed in the following sections.

a. Congressional Intent

The 1934 Act was crafted during President Roosevelt's New Deal program to nationalize the economic infrastructure during a time when the radio was gaining importance as a national communication forum.[126] Generally, the Act was created

120. *Id.* § 606(c).

121. *See id.*

122. Michael Socolow, *In a State of Emergency, the President Can Control Your Phone, Your TV, and Even Your Light Switches*, REASON (Feb. 15, 2019), https://perma.cc/8F38-XX3S ("The law permits the White House to take over *any* device that emits radiofrequency transmissions. In 2019, that's everything from your implanted heart device to the blow dryer for your hair.").

123. *But cf. Emergency Control of Electromagnetic Radiating Devices: Hearing on S. 537 Before the S. Comm. On Interstate and Foreign Com.*, 82d Cong. 14 (1951) (statement of Senator Warren Magnuson, Washington) (suggesting that a vast variety of things would fall within the proposed electromagnetic spectrum that are used in our American scientific and medical life), *with Hearing on S. 537* at 19-20 (statement of General Ankenbrandt) (suggesting that many things would not fall within the proposed spectrum).

124. *See generally* WHITE HOUSE CYBERSPACE POLICY REVIEW, *supra* note 13, at C-13; Opderbeck, *Cybersecurity and Executive Power*, *supra* note 104 at 831. For another summary of the Act's history during this early period, see Opderbeck, *supra* note 11, at 10-15.

125. The Congressional testimony does at least suggest an intent to foresee advancements in technology and the need to cover situations in the future. *See generally Hearing on S. 537*, *supra* note 123.

126. Opderbeck, *supra* note 11, at 16-17.

for the purpose of regulating wire and radio communications.[127] The Federal Communications Commission (FCC) was established under the Act to execute and enforce any applicable rules and regulations for such communications.[128] One of the main purposes for the Act was national defense.[129] Section 606(c) of the Act furthers this purpose as an emergency provision that grants the President broad powers over communications when required for the national defense.[130]

This emergency power, however, was never meant to be boundless. The legislative history of section 606(c) shows that Congress intended to carve out *systems* and daily use or *personal devices* from the confines of the Act. These two very important exclusions, analyzed below, work to limit the provision's application to the internet.

To start, the term *systems* was deliberately excluded from section 606(c) when it was initially codified as law in 1934; the provision was limited to address only *stations*.[131] Congressional testimony reveals that the term *systems* was excluded because it was thought to confer too much authority on the President to shut down entire telephone and radio systems.[132] Instead, the term *stations* was adopted and remained in the text after the 1951 amendment.

Next, Congress adopted the term *device*, but with limits. The 1951 amendment, the last amendment to section 606(c), is arguably most important for today's discussion of an internet shutdown because it sheds light on the meaning of the term *device*. At the time of the amendment, President Truman declared a state of emergency for the Korean war. It was against this backdrop that the Department of Defense (DoD) proposed broadening the scope of section 606(c).[133] To this end, the DoD proposed adding the term *device* as a means of broadening the President's powers to control radio and wire communications during an emergency.[134] The exact *devices* that would fall within the provision's purview became the subject of substantial debate in Congress. Hearing testimony shows that the term *device* ultimately comes with qualifications to limit its scope.

---

127. *See* 47 U.S.C. § 151 (2019).
128. *See id.*
129. *Id.*
130. *See* 47 U.S.C. § 606(c). Before the 1951 amendments, this provision read as follows:

> Section 606(c), War Emergency – Powers of the President. Upon proclamation by the President that there exists war or a threat of war or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communications and the removal therefrom of its apparatus and equipment, or he may authorize the use or control of any such station and/or its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.

Hearing on S. 537, *supra* note 123, at 8 (statement of Maj. Gen. Francis Ankenbrandt, Director of Communications, U.S. Air Force).
131. Opderbeck, *supra* note 11, at 17-18.
132. *Id.* at 17.
133. *See Hearing on S. 537*, *supra* note 123, at 8 (statement of Maj. Gen. Ankenbrandt).
134. *See id.*

When the amendment was first proposed to Congress, the language included any "*device* . . . capable of emitting electromagnetic radiation between ten thousandths and one hundred thousand megacycles per second which might assist any foreign country in an attack upon the United States . . . ."[135] Throughout the Congressional testimony, it was clear that Congress was hesitant to include common daily use devices of the American people. Major General Francis Ankenbrandt, Director of Communications for the United States Air Force, testified on behalf of DoD attempting to alleviate Congress' concerns. He assured Congress that although most electronic devices might "technically" fall within the purview of section 606(c), since they give off radiation within the amendment's spectrum, they would still be excluded under the purpose of the bill.[136] Expounding on this claim, he testified that televisions,[137] police radio stations,[138] cab company broadcasting,[139] and low power mobile devices,[140] such as amateur radios,[141] would not fall within the purpose of the bill. According to Ankenbrandt, this was because the radiation from such devices were not considered useful for navigational purposes. Ankenbrandt clarified that the bill would only apply to those fixed[142] devices that were capable[143] of becoming "homing devices" for aircraft and missile attacks by a hostile nation.[144] As a result, Congress amended section 606(c) to state, "any device . . . which is suitable for use as a navigational aid beyond five miles. . . ."[145]

Congress added the qualification of "beyond five miles" to further emphasize that everyday devices of the American people would not fall under the bill. This acknowledgement is highlighted in the testimony of Mr. David Smith, Vice Director of the Engineering, Radio and Television Manufacturers Association (the

135. *Id.*

136. *See id.* at 19-20.

137. *See id.* at 20-21. Senator Magnuson even specifically asks about television sets falling within the purview of the proposed emergency provision, to which he cautions, "we want to be sure that we do not stop America's entertainment." *See id.* at 20. In response, Gen. Ankenbrandt states that a television may not emit the type of radiation required (although it is unclear if he clarifies this point later in his testimony) and that even if it did it would not fall under the terms of the provision since it is not something "deemed necessary to minimize or prevent navigational aid to a foreign enemy." *See id.* 20-21. 20-21.

138. *See id.* at 22.

139. *Id.*

140. *Id.* (statement of Mr. Curtis Plummer, Chief Engineer, Federal Communications Commission) (claiming that "low power mobile devices are intermittent, which makes it much harder to use them for navigational assistance, whereas a broadcast station, for instance, is on all the time at relatively high power").

141. *Id.* (statement of General Ankenbrandt).

142. *See id.* at 10; *see also id.* at 34-36 (statement of Mr. W. R. G. Baker, Director of Engineering, Radio-Television Manufacturers Association).

143. *See id.* General Ankenbrandt pointed out that while many of the devices he excepted from the statute might be "capable" under certain conditions of radiating, to fall under the provision a device would need to be radiating *and* be useful for the purpose of being a homing device that the enemy could use. *See id.* (statement of General Ankenbrandt).

144. *See id.* at 10, 25.

145. 47 U.S.C. § 606(c); *see also Hearing on S. 537*, *supra* note 123, at 8-11.

Association). Mr. Smith elaborated on the testimony of General Ankenbrandt and stressed the importance of carving out exceptions for everyday devices. He warned that without qualifying language on devices, an electric razor, electric light, telephone, oil heater, radio, television set, or practically anything involving power could fall under the scope of the provisions, and that was not the intent.[146] As a remedy, he proposed some limitation on how far a device could be detected. He claimed that all of the daily use or everyday devices (literally millions of them) would not be detectable more than a few feet, or perhaps a few hundred feet.[147] This concept of creating a distance limitation on the radiation emissions was then solicited in a subsequent letter to Congress from the Association.[148] The letter offered two proposed amendments that included a "five mile" limitation.[149] Congress ultimately accepted this additional limitation for *devices* in the final section 606(c) still on the books today.[150]

Applying this congressional understanding of section 606(c) to today's world of electronic saturation, there can be no practical application to personal computing devices due to their inability to be "suitable for use as a navigational aid beyond five miles."[151] Notwithstanding the fact that mobile devices likely would not fall within the intended meaning of section 606(c),[152] the practical way an enemy could use personal devices today as a navigational tool is to access GPS information, cell site location information (CSLI), or other information content on the device itself. Information or data content, however, would obviously not qualify as radiation.

This might, however, leave open the possibility that the President could shut down GPS and CSLI collection devices or stations that work with personal devices to create that information in the first place, like satellites and cell towers. Then the question still remains whether those devices—satellites and cell towers—are radiating in a nature that proves useful as a potential homing device for the enemy to

146. *Hearing on S. 537*, *supra* note 123, at 54 (statement of Mr. David Smith, Vice Director of Engineering, Radio, and Television Manufacturers Association).

147. *Id.*

148. *See id.* at 92-94 (Comments from Radio-Television Manufacturers Association).

149. *See id.* The Association proposed changes to section 606 to qualify *devices*, in that, the devices be suitable for use as a navigational aid "beyond five miles." *See id.* at 92-94. The Association thought that this qualification would achieve the objective of giving the Executive the powers needed for national defense but limit the ability to control *all devices,* most especially those "not usable for navigational aids." *See generally id.* at 92-94. The Association concluded that such "limitations upon the executive power are the minimum needed for the protection of our ordinary pursuits against unnecessary invasion." *Id.* at 93.

150. *Cf.* 47 U.S.C. § 606(c). The proposed amendment that most closely represents the current version was recommended by Eugene M. Zuckert, Assistant Secretary of the Air Force. *See Hearing on S. 537*, *supra* note 123, at 84. His proposal was the only other proposal offered during the hearings that also included the qualifying language that devices were limited to those suitable for use as a navigational aid beyond five miles. He stated in his letter with the proposal that he believed the amendment would address the concerns of the prior testimony, most likely referring to the testimony of General Ankenbrandt and Mr. Smith. *See id.*

151. 47 U.S.C. § 606(c).

152. *See supra* notes 140-142 and accompanying text.

carry out an aircraft or missile attack.[153] The answer to this question is outside the scope of this paper, though. Nevertheless, it is sufficient here to say that Congress has clearly signaled that section 606(c) does not include those primary daily use personal *devices*, which today would undoubtably include personal computing devices.

In sum, taking into consideration the two carve out exclusions of *personal devices* and *systems*, it becomes difficult to argue that section 606 of the Communications Act gives the President the power to shut down the internet, which is exactly made up of *personal devices* connected through a network *system*. Put differently, Congress' implied and express exclusions to the Act effectively makes up the very definition of the internet; Congress effectively excluded the internet. It follows then that if a court were to interpret the plain language of the statute, the internet would be excluded.[154] Similarly, it follows that the President's ability to shut down the internet under this statute is not within the zone of maximum authority under the *Youngstown* analysis because there is no express authority from Congress under this provision for the President to shut down the internet. At this point it is even unclear whether the President could act within the "zone of twilight," as congressional intent implies otherwise.

The question remains then whether the President might be acting within the last two zones of authority—the "zone of twilight" or the "lowest ebb"— when directing an internet shutdown. The FCC's renewed understanding of government internet regulation and interpretations of the Communications Act and 1996 Telecommunications Act points to the lowest ebb of presidential authority, which is discussed in the next section.

b. Agency Interpretations

Congress created the FCC to serve as the sole body with the authority to make recommendations to Congress regarding national telecommunications.[155] Accordingly, the FCC was given rulemaking and regulatory interpretation authority in this space.[156] The FCC proposed the first significant overhaul of telecommunications law with the Telecommunications Act of 1996 (1996 Act).[157] The 1996 Act amended portions of the Communications Act and addressed the

153. Perhaps one could argue that the intent could be extended to cover a homing device for a modern-day cyber-attack. Even so, the shutdown of these devices might not offer any advantage in the information age.

154. When courts determine the plain meaning of a statute, courts give the terms their "ordinary, contemporary, and common meaning," absent an indication from Congress otherwise. *See, e.g.*, *United States v. Powell*, 680 F.3d 350, 355 (4th Cir. 2012). Both the plain meaning and legislative history should demand exclusion of the internet from the purview of section 606(c).

155. *See* 47 U.S.C. § 151; Papers of Franklin D. Roosevelt, Feb. 26, 1934 *Message to Congress Recommending Creation of the Federal Communications Commission*, AM. PRESIDENCY PROJECT, https://perma.cc/FY82-8GKV.

156. *See, e.g.*, 47 U.S.C. § 159 (discussing the FCC's ability to collect fees to recover costs of its rulemaking authority).

157. Fed. Commc'ns Commission, *Telecommunications Act of 1996*, https://perma.cc/Y9N4-Y3RC.

main issue of promoting competition and reducing regulation in telecommunications.[158] The internet, however, was minimally addressed. The Act simply reiterated that it was the policy of the United States "to promote the continued development of the Internet . . . preserve the vibrant and competitive free market that presently exists for the Internet . . . unfettered by Federal and State regulation."[159] The term "interactive computer service" was also introduced to mean any service or system that provides access to the Internet.[160] Notably, section 606 of the Communications Act remained unchanged after the 1996 Act amendments.

The apparent absence of internet regulation evident by the 1996 amendments was no oversight. The FCC's desire to avoid government internet regulation had been a growing trend moving into the 1996 amendments as the internet was developing. Through a series of prior Commission opinions, the FCC established that the internet generally does not fall within the consideration of the Communication Act.[161] The FCC established this in a series of decisions known as the *Computer Inquiries*.[162] The Commission established in those cases that "enhanced services," including computer processing applications used to act on content, code, protocol and other aspects of a subscriber's information are not regulated under the Act.[163] The FCC thought that the internet would most certainly fall within this definition of "enhanced services."[164]

Although the decisions in the *Computer Inquiries* cases were made prior to the common usage of the internet, this distinction was maintained in later FCC decisions, federal court decisions, and the Telecommunications Act of 1996.[165] This historical development of the terms is succinctly laid out in the 2018 FCC order, "Restoring Internet Freedom," which returns the internet to its original "light-touch" regulatory framework that still operates today.[166] A brief summary of this development makes clear that courts would have to interpret the internet as not falling under the regulatory scheme of either the Communications Act or the 1996 Telecommunications Act. Effectively then, this forecloses the President's ability to shut down the internet under these authorities.

Congress' enactment of the Telecommunications Act in 1996 maintained the distinction between enhanced services (or information services) and

158. Telecommunications Act of 1996, P.L. No. 104-104, 110 Stat. 56 (1996).

159. Telecommunications Act § 230 (b)(1)-(2). The Internet was very minimally mentioned in the amendments made by the Telecommunications Act. It was included under Title I that outlined general purposes and definitions and protection for private blocking and screening of offensive material (§ 230). The Supreme Court has even recognized this significance aspect of the Telecommunications Act and that its "major components have nothing to do with the internet." *Reno v. ACLU*, 521 U.S. 844, 857-59 (1997).

160. *See id.* at § 230(e).

161. Restoring Internet Freedom, FCC Rcd. 17-166, WC Docket No. 17-108, 3-8 (Jan. 4, 2018).

162. *Id.* at 3.

163. *Id.* at 3-4.

164. *See id.* at 3-8.

165. *See id.* at 3-8.

166. *See id.* at 2.

telecommunications services that was put forth in the early FCC decisions.[167] By maintaining this distinction, Congress showed their intent to not abrogate the prior interpretation of the Communications Act's scope. Thus, the 1996 Act did not amend the Communications Act to include the internet under its regulatory scheme. Rather, the 1996 Act provided additional measures for the FCC to take in regulating telecommunication services and drew a bright line between lightly regulated "information services."[168]

In fact, the very purpose of the 1996 Act was to promote overall competition and *reduce* regulation.[169] As mentioned above, Congress even made a specific finding that the internet was to remain "unfettered by Federal and State regulation."[170] The Supreme Court recognized Congress and the FCC's intent to maintain a distinction with the internet as an "enhanced service" (as established in the *Computer Inquiries*) or an "info service" in 2005.[171] This Supreme Court decision, *Brand X*, highlighted the stance of Congress and the FCC to keep the internet unfettered by federal and state regulation.

However, the status quo over internet regulation was challenged when then-President Obama called on the FCC in 2014 to "reclassify consumer broadband service under Title II of the Telecommunications Act," which would place the internet under a regulatory scheme.[172] In response, the FCC adopted the *Title II Order* that made this reclassification.[173] The *Title II Order* effectively called into question the previous understanding of internet regulation under the Telecommunications and Communications Acts.

Prior to the adoption of the 2018 FCC Restoring Internet Freedom order, this shift in regulation brought about by the *Title II Order*—directed by the President and implemented by the FCC—might support the contention that Congress intended for the internet to be subject to regulation under both Acts. Despite this possible support for such an interpretation, it is critical to note that Congress was not at the helm of this sea change. In fact, this was a clear shift away from prior congressional intent. In 2016, the D.C. Circuit nonetheless upheld the *Title II*

167. *See id.* at 4.

168. *See id.*

169. Telecommunications Act of 1996, P.L. No. 104-104, 110 Stat. 56, Preamble (1996).

170. Telecommunications Act § 230(b)(2); Restoring Internet Freedom, FCC Rcd. 17-166, WC Docket No. 17-108, 2 (Jan. 4, 2018).

171. *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 992-93 (2005) ("Congress passed the definitions in the Communications Act against the background of this regulatory history, and it may be assumed that the parallel terms 'telecommunications service' and 'information service' substantially incorporated the meaning of "basic" and "enhanced service, as the Commission has held."). While the Court in *Brand X* found ambiguity over the definitions of a telecommunications service and information service, it held that the Commission has the discretion to fill the statutory gap. *See id.* This gap has now been filled through the Commissions' recent Restoring Internet Freedom order. *See* Restoring Internet Freedom, at 246.

172. *See* President Obama, Statement on Net Neutrality (Nov. 10, 2014), https://perma.cc/ACV5-MJ3V.

173. *See* Fed. FCC Releases Open Internet Order on Remand, Declaratory Ruling, and Order, 81 Fed. Reg. 19737 (Apr. 13, 2015), 81 Fed. Reg. (Dec. 21, 2016).

Order in *US Telecom Associate v. FCC*, concluding the agency had the authority to reclassify internet service under administrative law theories.[174]

Shortly after, the FCC relooked these actions. In 2017, the FCC issued a notice of proposed rulemaking, proposing a return to its original interpretation of the Act and to reinstate the classification of the internet as an information service that would not fall within the regulatory scheme of Title II.[175] In January 2018, the FCC issued its Restoring Internet Freedom order, declaring its reinstatement of the internet as an information service, effectively returning the FCC back to its original understanding of internet regulation.[176] Thus, the FCC ended public-utility regulation of the internet pursuant to the Acts and went back to reinforcing all previous interpretations of regulating the internet.

Consequently, any lingering authority the President may have been able to point to under a broad interpretation of section 606 of the Communications Act to shut down the internet has now been decisively removed. Recall that section 606(c) allows the President in a time of emergency to suspend or amend "rules and regulations applicable" to such "stations and devices;"[177] however, the 2018 FCC order clearly establishes that there are no government-imposed "rules and regulations" to suspend or amend. Therefore, section 606 becomes less viable as a source of Executive authority over the internet.

In summary, the FCC's storied past with internet regulation shows that Congress did not provide express authority to the Executive in this area. Quite the opposite, Congress appears to have already spoken about unfettered government regulation of the internet that is not to be covered under the Acts.[178] The Executive, at a minimum, would then be acting inconsistent with the Telecommunications Acts by instituting an internet shutdown. This would put the Executive's authority to shut down the internet squarely within *Youngstown's* "zone of twilight," and dangerously nearing the edges of the lowest ebb of authority. Whether the Supreme Court might take this same position is discussed in the analysis that follows.

3. The Internet is Different

In 2012, Professor David Opderbeck wrote an in-depth article outlining the executive power in cyberspace.[179] He asserted that "there does not appear to be a unified perspective on what 'cyberspace' represents, or what degree of control the Executive should be empowered to assert over it."[180] At the time, the Child

174. *United States Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016).

175. *See* Fed. Restoring Internet Freedom, 82 Fed. Reg. 25568 (June 2, 2017).

176. Fed. Restoring Internet Freedom, FCC Rcd. 17-166, WC Docket No. 17-108, 2 (Jan. 4, 2018).

177. 47 U.S.C. § 606(c).

178. By creating the FCC under its Article I lawmaking powers, Congress intended for the FCC to be able to speak for Congress through its rulemaking authority specifically provided by Congress in the Communications Act.

179. *See generally* Opderbeck, *Cybersecurity and Executive Power*, *supra* note 104.

180. *Id.* at 838.

Online Protection Act (COPA) cases only started to give us an idea about how the Supreme Court might stand with regard to domestic cyberspace.[181]

In 1997, the Supreme Court decided the first in a series of COPA cases.[182] In *Reno v. ACLU*, the Supreme Court found the challenged provision of the Communications Decency Act of 1996 unconstitutional because it created an overly broad burden on free speech carried out in the expanding "new marketplace of ideas" that is the internet.[183] Writing for the majority, Justice Stevens distinguished cyberspace; he viewed the internet as something unique in scope that has not had a long history of government regulation, unlike the broadcast industry.[184] Justice Stevens clearly made a marked distinction between the internet and radio or television, finding that it was not as "invasive" as radio or television nor was it a "scarce" expressive commodity that might militate toward tailored regulation.[185] Justice O'Connor's dissent, however, made this distinction even more black and white by noting that "the electronic world is fundamentally different" than the physical world.[186]

Years later, the Court again signaled in *Brand X* that the internet is different.[187] In that case, the Court confirmed the FCC's ability to make rules that could instill the light-touch approach to internet regulation.[188] Both the *Brand X* and *Reno* cases emphasize the Supreme Court's understanding that Congress intended for a lightly government regulated internet. The FCC takes this a step further in its 2018 Restoring Internet Freedom order and asserts that the internet should be altogether free from government regulation.[189] Presumably, the Supreme Court would now confirm this view if challenged based on an application of the traditional *Chevron* deference provided to an agency's interpretation of a statute as it did in *Brand X*.[190] Since the FCC acts as Congress' regulatory body in this area,

181. For a detailed discussion of these cases as they relate to cyberspace and the Executive's authority, see Opderbeck, *Cybersecurity and Executive Power*, *supra* note 104, at 833-37.

182. *See generally Reno*, 521 U.S. 844 (1997).

183. *See id.* at 882-85. In *Reno v. ACLU*, civil liberties organizations and library and publishing trade groups challenged the Communications Decency Act that "banned the use of 'any interactive computer service to display [obscene material] in a manner available to a person under 18 years of age,' and made it a crime to 'knowingly permit' the use of a telecommunications facility 'with the intent that it be used for such' purposes." Opderbeck, *Cybersecurity and Executive Power*, *supra* note 104, at 833 (citing *Reno v. ACLU*, 521 U.S. at 860).

184. *See id.* at 865-68.

185. *Id.* at 869-70. However, Justice Stevens' categorization of the internet as not as "invasive" may no longer be valid given today's information technology platforms and data practices.

186. *Id.* at 889-90 (O'Connor, J., dissenting) (distinguishing the physical world from cyberspace because "cyberspace allows speakers and listeners to mask their identities" and "[c]yberspace is malleable").

187. *See generally Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967 (2005) (giving deference to the agency distinction between internet services and other telecommunications services).

188. *See id.* at 992-93.

189. Restoring Internet Freedom, FCC Rcd. 17-166, WC Docket No. 17-108, 2 (Jan. 4, 2018).

190. *See Brand X*, 545 U.S. at 980. In *Chevron*, the Supreme Court "held that ambiguities in statutes within an agency's jurisdiction to administer are delegations of authority to the agency to fill the statutory gap in reasonable fashion." *Id.* "If a statute is ambiguous, and if the implementing agency's

the Court should view the FCC position on internet freedom as Congress' implied will. Thus, the Court would likely find the lowest ebb of *Youngstown* implicated. Whether the Court takes this as its final position may be fostered by its perception of the internet or cyberspace generally.

Fortunately, the Court has provided more insight into its perception of the internet or cyberspace. The Supreme Court has started to fill the gap on how it perceives or might perceive the internet or cyberspace through its analysis of technology advancements. In a series of recent Fourth Amendment cases concerning cell phones and corresponding surveillance tools (i.e., GPS or CLSI location tracking technology), the Supreme Court has firmly established that there is a clear distinction between digital technology and the physical world and that the two are not adequate for comparison.[191]

These Fourth Amendment cases show us that the Court believes that digital is different. Professor Paul Ohm has labeled this thought shift by the Supreme Court as "tech exceptionalism."[192] Under the idea of "tech exceptionalism," the Court would also likely be reticent to analogize *modern computing technologies* to technologies created in the radio era because they offer little adequate comparison. Additionally, this idea may further operate to bar certain aspects of government intrusion in modern technology that impacts daily life.

The Court not only views the technology in these cases as exceptional—in the sense that there is no modern-day physical world equivalent—but also that these personal technological devices (i.e., smart phones) have become a critical and indivisible part of Americans' everyday lives. In making this point, Chief Justice Roberts theatrically concludes in *Riley* that a smart phone has become almost a "feature of human anatomy" in the modern world.[193] He reiterates this point again when writing for the majority in *Carpenter*.[194] In that case, the Chief Justice expounds on this concept asserting, "cell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[195] This facet of smart phones leads the

---

construction is reasonable, *Chevron* requires a federal court to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is the best statutory interpretation." *Id.* (citing *Chevron, U.S.A., Inc. v. NRDC, Inc.*, 467 U.S. 837, 843-44 (1984)). *But see Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) (declining to apply full *Chevron* deference to an agency interpretation of a statute when faced with an opposing Presidential interpretation of the statute, although not specifying an alternate standard of review). Assuming there may be some modified version of *Chevron* deference applied by the Court if there was a contrary Presidential interpretation, the interpretation is still likely to go in favor of the agency when there is no specific statute that applies to the proposed Presidential actions, as would be the case here after a legislative history review of section 606. After *Franklin*, courts have also provided varying degrees of deference to the President depending on how the *Youngstown* analysis flushes out. *See* Amy L. Stein, *A Statutory National Security President*, 70 FLA. L. REV. 1183, 1211-214 (2018).

191. *See Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018); *Riley v. California*, 573 U.S. 373, 385 (2014); *United States v. Jones*, 565 U.S. 400, 417 (2012); *id.* at 428-431 (Alito, J., concurring).

192. Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TEC. 357, 399 (2019).

193. *Riley*, 573 U.S. at 385.

194. *See Carpenter*, 138 S. Ct. at 2220 (quoting *Riley*, 573 U.S. at 385).

195. *Id.*

Court to scrutinize the nature of the government intrusion into the location data collected from smart phone use. The Court found that the nature of the intrusion on privacy was greater when dealing with a device that is indispensable to participation in modern life, reasoning that daily smart phone usage shows the involuntary nature of CSLI location data.[196]

While these cases focus on a person's reasonable expectation of privacy related to location tracking information available from smart phone use,[197] it is not necessarily the location tracking that makes smart phones "indispensable to participation in modern society."[198] Rather, the inescapable reality is that a smart phone is indispensable to participation in modern society because of the internet. It is the internet that provides the services that allow for the participation in modern society.[199] Put simply, what makes the smart phone smart is the internet.[200]

Following this line of thinking, the Court would be rightly situated to adopt the view that the internet is indispensable to participation in modern society. As such, Executive intrusion upon the internet or a "seizure" by the Executive, would face considerable scrutiny by the Court, likely even outside a Fourth amendment context. The Court would also likely be highly critical of any interpretation that the radio era emergency powers of the Communications Act could be applicable to the very different technology that the internet and computing devices offer us today. If, on top of these concerns, you also add a First Amendment gloss, then the Court is sure to apply some level of heightened scrutiny when analyzing Executive authority over the internet.

4. A First Amendment Gloss

The Constitution requires the President to conform all his actions to his constitutional obligation to "take care that the laws be faithfully executed."[201] A constitutional violation would make any directive, regulation, or statute null and void. The First Amendment provides the largest shield against the emergency power sword in the case of an internet shutdown.

First Amendment implications surrounding cyberspace and an internet shutdown have been thoroughly discussed by legal scholars and civil liberties

196. *See id*. at 2218.

197. *But cf*. Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST SECURITY (June 27, 2018), https://perma.cc/NTG9-27QQ.

198. *Carpenter*, 138 S. Ct. at 2220.

199. One could argue that another aspect to the smart phone is the cell service that allows people to communicate; however, this might be challenged in today's information environment. In any case, the mere ability to make phone calls would not be found as exceptional by the court since telephones, without smart capabilities, were in existence and part of the Court's prior jurisprudence before it made the "tech exceptionalism" shift. For example, in *Katz* the Court had no issue with making an analogy to the physical world when discussing a phone booth. *See Katz v. United States*, 389 U.S. 347, 352 (1967).

200. *See, e.g*., Liane Cassavoy, *What Makes a Smartphone Smart*, LIFEWIRE (Sept. 28, 2019), https://perma.cc/ZFC9-DDQX. Today, Americans' primary way of accessing websites happens on mobile devices, such as smartphone and tablet devices. Freddie Blicher, *Mobile Analysis: Mobile Device Trends on Government Websites*, DIGITAL.GOV (Aug. 14, 2017), https://perma.cc/R9Z4-9FPM.

201. U.S. CONST. art. II, § 3.

activists alike.[202] Shutting down the internet or portions of networks most apparently implicate violations of freedom of speech, freedom of assembly, and freedom of the press. Nested within these rights, however, is the right to receive information and ideas. The Supreme Court in *Stanley v. Georgia* reiterated that the freedom of speech and press "necessarily protects the right to receive,"[203] and that this right to receive information and ideas is "fundamental to our free society."[204] The right to receive information and ideas is the right that would be implicated almost universally by American citizens if there was an internet shutdown.

When these important rights are at stake, Courts are especially willing to engage in more robust judicial review.[205] This is so even in the national security context. The Supreme Court has clearly established that the First Amendment cannot be ignored for the sake of national security. In *United States v. Robel*, the Supreme Court held that a U.S. person cannot be deprived of the fundamental right of association under the First Amendment in the name of national security.[206] The Court succinctly stated, "[it] would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties . . . which makes the defense of the Nation worthwhile."[207] The Supreme Court most recently solidified the Court's position on challenges to the First Amendment in the face of national security interests in *Holder v. Humanitarian Law Project*.[208] The majority in *Holder* affirmed that the Court "do[es] not defer to the Government's reading of the First Amendment" even when national security interests are at stake.[209]

The vast First Amendment implications involved in an internet shut down is what distinguishes it from other emergency powers that might, for example, seize property or direct land management, and thus places it squarely within the lowest ebb of presidential power. When outlining the parameters of the lowest ebb of

202. *See, e.g.*, Ruggiero, *supra* note 11, at 249-53. A 2018 Human Rights Council U.N. General Assembly Resolution was adopted affirming that the same human rights that people have offline must be protected online. *See* Human Rights Council Res. 38/7, U.N. Doc. A/HRC/RES/38/7 (July 17, 2018).

203. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (quoting *Martin* v. *City of Struthers*, 319 U.S. 141, 143 (1943)).

204. *See Stanley*, 394 U.S. at 564.

205. *See* Stein, *supra* note 190, at 1210.

206. *See United States v. Robel*, 389 U.S. 258, 271-73 (1967). "But in areas of protected freedoms, regulation based upon mere association and not upon proof of misconduct or even of intention to act unlawfully, must at least be accompanied by standards or procedural protections sufficient to safeguard against indiscriminate application." *Id.* at 282.

207. *Id.* at 264. *Id.* at 264. *Cf. Kennedy v. Mendoza-Martinez,* 372 U.S. 144, 165 (1963) ("The imperative necessity for safeguarding these rights to procedural due process under the gravest of emergencies has existed throughout our constitutional history, for it is then, under the pressing exigencies of crisis, that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action."); *Hamdi v. Rumsfeld,* 542 U.S. 507, 533 (2004) (holding that a citizen-detainee is entitled to due process rights even while engaged in a period of ongoing combat).

208. *See generally Holder v. Humanitarian Law Project*, 561 U.S. 1 (2010).

209. *See Holder*, 561 U.S. at 33-34 ("[T]he Government's 'authority and expertise in these matters do not automatically trump the Court's own obligation to secure the protection that the Constitution grants to individuals.'").

authority, Justice Jackson wrote at length about the dangers of executive control over civilian industries and other liberties even during wartime.[210] In doing so, Jackson signals that civil liberty implications will almost certainly tip the scales in the end against the Executive.

5. A Fifth Amendment Taking

A final constitutional argument against an internet shutdown is a Fifth Amendment violation. Most scholars posit that a Fifth Amendment takings claim for an internet shutdown would be defeated quickly.[211] One of the main arguments against a takings claim is that existing case law regarding seizures during national emergencies are viewed as temporary deprivations of property that do not vest any assets in the federal government to qualify as a taking under the law.[212] For the most part, this may be the case when talking about an internet shutdown.

Nevertheless, a violation of the Fifth Amendment is not out of the realm of possibilities, so it is worth mentioning here. A violation, arguably, could occur; it would just depend on how the internet shutdown was effectuated. If, for example, in the context of internet use via broadband (one of the most commonly used methods to access the internet) the government retained its spectrum use and directed other networks to cease operations on the spectrum,[213] and even perhaps also took control of associated cables, servers, routers, or data centers, the additional bandwidth that is freed up or access to those servers, routers, data or metadata would potentially vest a benefit upon the government. Today it is common for the market to charge higher prices for higher bandwidth speeds, it serves as a valued commodity. Access to servers, routers, and the use of data or metadata is similarly valuable. Spectrum licensees, ISPs, or data owners or brokers might then have standing to file temporary injunctions in court since these private entities retain rights in these commodities, such as a spectrum licensee's right in spectrum use.[214] Arguably, if the motions for injunctions also allege ancillary First Amendment implications then courts are almost surely to come out in favor of the ISPs, as explained above.[215] A slew of litigation might then make an emergency shutdown or isolation impossible to achieve its necessary effects.

---

210. *See* Opderbeck, *Cybersecurity and Executive Power*, *supra* note 104, at 814.

211. *See, e.g.*, Brunner, *supra* note 4, at 418.

212. *Id.*

213. First, it was Congress that directed the FCC to auction off spectrum use; second, auction winners do not actually own the spectrum, but merely the license to operate for cellular services. *See* Farber, David J. and Gerald R. Faulhaber, *Spectrum Management: Property Rights, Markets, and The Commons*, 1-3 (2002). Even so, there are cognizable rights in spectrum use by licensees. *See generally NextWave Personal Comm. Inc. v. FCC*, 254 F.3d 130 (D.C. Cir. 2001) (holding that a spectrum license is considered an asset of the firm). In sum, there is a good case to show property rights in both the physical infrastructure of the internet controlled by ISPs or other private entities and also the spectrum use controlled by cellular license holders.

214. *See, e.g.*, sources cited *supra* note 213.

215. *See, e.g.*, *Ctr. for Democracy & Tech v. Pappert*, 337 F.Supp. 2d 606, 611 (E.D. Pa. 2004) (finding a statute requiring ISPs to block content was a prior restraint on speech and thus violated the First Amendment).

Admittedly though, a Fifth Amendment takings claim is speculative at best; however, raising the potential issue helps illustrate the acute point that an internet shutdown has a vast array of possible constitutional implications depending on how it is carried out or for what purposes. An effective and timely national security response then may be difficult to achieve based on considerations for the protection of fundamental rights and consequent time-consuming litigation.

IV. MOVING FORWARD: A PROPOSAL FOR NATIONAL CYBER QUARANTINE

The arguments above are intended to show that if the President were to order an internet shutdown during a declared cyberspace emergency he would ultimately be "choosing a different and inconsistent way of his own."[216] Such an order would be contrary to congressional intent under the Communications Act and FCC (Congress' communications body with the authority to speak for Congress through its rulemaking authority) interpretations of internet governance. Therefore, Congress has not left internet shutdowns "an open field" to provide the President the benefit of the "flexible tests" under the second category or zone of twilight.[217] Under the third category, or lowest ebb of authority, the President's actions could then only be found constitutional if an internet shut down was "within his domain and beyond control by Congress."[218] The discussion above shows that this too may not be the case, most especially when adding concerns over violations of fundamental rights to the analysis.

Fundamental rights implications can effectively work to close the door on any further claims of Presidential authority in this area. As Justice Jackson summarized in *Youngstown*, "this leaves the current seizure to be justified only by the severe tests under the third grouping, where it can be supported only by any remainder of executive power after subtraction of such powers as Congress may have over the subject."[219] That subtraction of powers may also come in the form of explicit constitutional constraints on the President, which "leave[s] presidential power most vulnerable to attack and in the least favorable possible constitutional postures."[220]

This perhaps leaves open the question of whether broader emergency authorities such as IEEPA could be used instead of section 606 of the Communications Act to effectuate an internet shutdown.[221] While an in-depth analysis to this question exceeds the extent of this paper, IEEPA still seems a poor fit to answer this question after a brief overview of its authority.

---

216. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 587, 639 (1952) (Jackson, J., concurring).

217. *See id.*

218. *See id.* at 640.

219. *Id.*

220. *Id.*

221. An in-depth analysis to this question exceeds the extent of this paper. For further discussion on IEEPA, see Brunner, *supra* note 4, at 406-08.

Generally speaking, IEEPA's broad in scope nature, focus on sanctions, and procedures that run in the background to effectuate its authority under the Office of Foreign Assets Control (requiring a case-by-case analysis) would make it an equally ill-equipped tool to assert Executive authority over the internet or cyberspace.[222] These factors make it even less suitable in the face of civil liberties concerns.[223] It is also important to consider the fact that the only case to invalidate domestic asset seizure by the President is *Youngstown*, which reaches a similar result as is argued here in an internet shutdown situation. IEEPA's application, therefore, as a source of authority becomes shaky at best. In the end, it is likely enough to say that the implication of fundamental rights would be a significant bar to any assertion of IEEPA or other broader emergency authority in this area.[224]

Where does this all lead the United States with respect to its cyberspace emergency authorities? Simply put, the state of the law is in an uncertain place. And, this uncertainty is reason enough to warrant new proposals that can provide for "clear guidance and an enhanced ability to rapidly execute National level decisions for response options to sophisticated attack," which is what was originally called for to address a massive cyber-attack over a decade ago.[225]

A. The Current Incident Response Framework

To address the threat of a national cyber-attack, the government has produced multiple assessments and issued guidance and directives over the years in an attempt to mitigate vulnerabilities, improve defenses and responses, and predict

222. *See generally About Office of Foreign Assets Control (OFAC)*, DEP'T OF TREASURY, https://perma.cc/KL87-X68N; U.S. DEP'T OF THE TREASURY, OFAC FAQS: GENERAL QUESTIONS, https://perma.cc/CHT6-7LBN. IEEPA does not work in a vacuum. The sanctions that it authorizes have to operate under the guidance and procedures of the Office of Foreign Assets Control, part of the United States Treasury Department, which requires a case-by-case analysis for all sanctions. *See id.* This authority may be sufficient to ban individual internet users if they are engaged in foreign property transactions or have materially benefited from those transactions. *See* sources cited *supra* notes 36-38 and accompanying text. But in the majority of cases for an internet shut down, the issue is not sanctions against individual users, nor is it targeting those who knowingly engage in foreign transactions. Thus, this authority seems impractical for use to effectuate an internet shutdown.

223. Interpreting IEEPA broadly enough to claim it provides the authority for an internet shut down would also trigger the very same arguments against why there is no domestic terrorism statute in the United States. *See, e.g.*, Bobby Chesney, *Should We Create a Federal Crime of 'Domestic Terrorism'?* LAWFARE BLOG (Aug. 8, 2019), https://perma.cc/M4EZ-3SGA. Such an interpretation would raise significant concerns over the infringement on rights of U.S. persons, such as the freedom of speech, freedom of association, and due process concerns. *See id.*

224. Another broad source of emergency authority that one might argue for use in the area of a cyberspace emergency to address a foreign threat is the Immigration and Nationality Act of 1952, but which would likely still fail to provide sufficient authority due to similar reasons as IEEPA. *See generally* INA, 8 U.S.C. §§ 1100-1537 (2019). Pursuant to the INA, one would also have to argue that a foreign malicious code is analogous to the entry of aliens in the United States, and by the terms of the statute aliens means a person. *See id.* at § 1101(a)(3). For further discussion on the INA, see Brunner, *supra* note 4, at 408-10.

225. *See NSTAC*, *supra* note 12.

the nature of massive attacks.[226] As a result, the government has developed what one might consider to be a rather robust framework for cyber incident response.[227] Most recently, Presidential Policy Directive (PPD)-41, *U.S. Cyber Incident Coordination*, was published in July 2016 and attempts to set forth principles and a general architecture for responding to massive cyber-attacks.[228] Six months after PPD-41 was published, the federal government supplemented it with the National Cyber Incident Response Plan (NCIRP).[229] The NCIRP established a more comprehensive framework for responding to a cyber-attack, with a focus on protecting critical infrastructure.[230]

Notwithstanding the overall breath of the current framework, it still remains problematic for three main reasons. First, the framework does not explicitly address a "kill switch" authority or a quarantine, isolation, or internet shutdown process, rather it merely lists the controversial section 706 of the Communications Act of 1934 as a source of authority.[231] Second, despite the interconnected nature of the U.S. cyber infrastructure, these government efforts leave private entities and individuals outside of its scope.[232] Considering the majority of U.S. cyber infrastructure is held in private hands, this is a significant gap of the framework. Finally, the entire plan is based on coordination and voluntary cooperation; there is no mechanism for the government to order actions in the face pressing time constraints or resistant private entities. Addressing these gaps, albeit a daunting challenge, requires Congress and executive agencies to revisit and revise the response plan framework or implement clear cyberspace emergency authorities to ensure the United States is properly equipped to defend and recover from any massive cyber-attacks.

B. Proposals for Improving Incident Response and National Cybersecurity

1. Amending Section 606(c)

The hands-off approach to addressing a "kill switch" authority in the current response framework seems reasonable when considering the overwhelming lack

226. *See id.*

227. *See generally* DEP'T OF HOMELAND SEC., NATIONAL CYBER INCIDENT RESPONSE PLAN (2016) [hereinafter NCIRP], https://perma.cc/N42Y-KPW4. For a complete laundry list of referenced authorities making up the incident response framework, *see id.* at Annex A. Other major authorities for incident response include: Executive Order 13618, Executive Order 13636, Cybersecurity Act of 2015, and the National Infrastructure Protection Plan (NIPP) (updated in 2013 to include cyber considerations). *See id.* DEP'T OF HOMELAND SEC., CISA, NATIONAL INFRASTRUCTURE PROTECTION PLAN, https://perma.cc/7ZLA-KHQL.

228. *See* Presidential Policy Directive on United States Cyber Incident Coordination (PPD-41), Comp. Press. Doc. (Jul. 26, 2016), https://perma.cc/G4NH-WFSN.

229. *See* NCIRP, *supra* note 227.

230. *See id.*

231. *See id.* at Annex A.

232. *See id.* at 10 ("When a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort."). The current list of critical infrastructure lists sixteen different sectors, covering a large swatch of private entities, making it somewhat more difficult to envision on its face what sectors or entities are not covered. *See* PPD-41, *supra* note 228. Yet, in the end, the framework still does not address a vast majority of large and small businesses or individuals.

of appetite in the United States for such a sweeping Executive authority. The failed legislative attempts concerning cyberspace emergency authorities from 2010 through 2012 highlight this point best. Renewed legal commentary after the border wall emergency also highlights the dangers and opposition to having such broad and sweeping authority. Further, current legislative attempts similarly echo this sentiment.

On June 2019, Senators Rand Paul (R-KY) and Ron Wyden (D-OR) introduced the Reforming Emergency Powers to Uphold the Balances and Limitations Inherent in the Constitution (the REPUBLIC Act).[233] If enacted, the bill would repeal what is considered by some to be "one of the most dangerous emergency powers lurking in the U.S. code: Section 706 [47 U.S.C. 606] of the 1934 Communications Act."[234] This contention has merit.

Section 606 is more dangerous than it appears on its face because the scope of the authority that it may provide the Executive is so contested. If the authority were to be relied upon by the Executive, it would face immense constitutional scrutiny (and likely partisan critique as well). But, if left with no alternatives, the Executive may be forced to invoke its power if the provision remains on the books and the situation dictates action. Thus, based on the discussion above, the congressional effort to repeal this authority seems prudent and wise, most especially because repealing this authority would clarify to the national security field and public that the use of section 606(c) by the Executive to order any form of emergency internet shutdown would violate the Constitution's separation of powers. Further, the question of authority would no longer be left unanswered or open for broad interpretation, thereby limiting any uncertain, sweeping, or contested power grabs by the Executive. The end goal should be to ensure that the nation is not left in a place of uncertainty during times of emergency. Repealing section 606(c) is a start toward accomplishing this goal.

On the other hand, merely repealing this authority without any further clarification regarding the Executive's authority is shortsighted and would leave a large gap in this area of the law. Accordingly, an alternative proposal is to amend section 606(c)—rather than repeal it wholesale—to clarify the scope of the emergency powers. Under such a proposal, the provision could be more narrowly tailored to define its scope, impose significant limits on the Executive, and provide due process rights to those entities potentially affected by the authority. Perhaps, however, the tide already shifted away from that very tactic since this is what was similarly proposed in the PCNAA in 2010 and was unsuccessful in garnering support.[235] More importantly, this proposal may fairly run counter to the current FCC position on internet governance and continue to present significant harmful implications on fundamental rights.

233. *See* REPUBLIC Act, S. 1809, 116th Cong. § 3 (2019).

234. *See* Healy, *supra* note 11; *see* Goitein, *supra* note 11. The bill also imposes other limits on Executive emergency powers. *See* REPUBLIC Act.

235. *Cf.* Protecting Cyberspace as a National Asset Act, S.3480, 111th Cong. § 249.

2. Strengthening the Decentralized Approach

Another potential approach is to continue with the status quo of decentralized private sector authorities in cybersecurity and provide additional mechanisms to strengthen defenses. One method to achieve this would be for legislative or regulatory efforts to impose requirements directed at critical infrastructure entities, ISPs, or data exchange points to implement sector approved methods at their level to effectuate a targeted internet shutdown in case of an emergency. This method still heavily relies on voluntary cooperative efforts, but is more realistic to achieve because, to some extent, this proposal is already underway within many of the critical infrastructure entities.

For example, in 2016 the U.S. Communications Sector Coordinating Council published information about its state of cybersecurity when requested by the National Institute of Standards and Technology (NIST).[236] In its 2016 letter to NIST, the Council stated that entities within the sector were already developing their network architectures to be able to "quarantine data or limit an attacker's access to resources outside of a specific data set, all of which helps limit the impact of an attack."[237] In that case, the sector entities were employing Software Designed Networks that separated the physical network control from the data plane allowing the intermediate data plane to be directly programmable and offer a layer of protection from the underlying network.[238]

Another method that could be used to strengthen the decentralized approach is for legislation to permit certain types of capabilities or cyber mechanisms that are used and developed by the private sector to decrease vulnerabilities, thereby contributing to the protection of the nation's cybersecurity as a whole. Such programs have previously been advocated for in the form of implementing bug bounty programs and providing incentives for the use of such programs.[239] Although bug bounty programs are nothing new, incentives and regulations could be modified to improve efficacy of these programs and increase efforts by the private sector to monitor their own systems, particularly critical infrastructure.[240] Oversight could be provided by the Commerce Department, and specific limits could be placed on bounties, methods of researching, and reporting on foreign actor malicious cyber activity and malicious tools.[241]

Providing for these authorities is considered by some to be equitable given the U.S. government has mass resources in this area and engages in the Vulnerabilities Equities Program to determine whether or not to alert the public

236. *See, e.g.*, Letter from U.S. Commc'ns Sector Coordinating Council, *supra* note 74.

237. *Id.* at 8.

238. *See id.*

239. *See generally* Joseph Marks, *Here's What Government Gets Wrong About Bug Bounties*, NEXTGOV (Apr. 4, 2018), https://perma.cc/2MMB-P3T2; Center for Democracy & Technology, "The Cyber" Hard Questions In the World of Computer Security Research, CDT (Mar. 2017) https://perma.cc/JQ5Q-LRQB (discussing an overview of bug bounty programs and options to use such programs to increase cybersecurity in the private and government sector).

240. *See id.* at 31-38.

241. *See generally id.*

to known vulnerabilities or use such vulnerabilities in their own defense.[242] In any case, the inequitable allocation of resources and information weigh strongly in favor of providing the private sector with additional legal methods and more incentives to identify and combat vulnerabilities in their own systems, whether it is through a bug bounty program or some other means.

Although the decentralized approach to improving cyber incident response seems most palatable to the American public, and it allows for more inclusion of the private sector, it still has its faults. Solely focusing on strengthening the decentralized approach to cybersecurity fails to take into account the very real possibility that the nation may be faced with a situation that requires the government to quarantine, isolate, or shutdown computers or portions of the internet or networks in a time of emergency caused by a massive cyber-attack. Not planning for an eventuality will make the conclusion inevitable. One need not look any further than the handling of the novel 2019 coronavirus to understand how true this can be. Not planning or having clear authorities for a cyberspace emergency at the national level will also create a recipe for panic among the American people if there is a massive wide-spreading cyber-attack and no clear roadmap or centralized authorities to navigate it.

3. Establishing A National Cyber Quarantine Authority and a "Healthy" Cyber Nation

In light of the above proposals and their shortcomings, a recommendation that might be able to address many of the concerns discussed throughout this paper is for the United States to supplement this decentralized approach with an explicit national cyber quarantine authority. Such an authority may offer a more balanced approach to this issue that can provide tools in a measured and limited way that is both clear and allows for public participation in the process. Again, Congress need not look far to find a similar approach already in existence in the United States: The Health and Human Services/ Center for Disease Control (CDC) Quarantine Program.[243]

The CDC federal quarantine rule serves as a starting-point template for implementing similar authorities and a corresponding program that is explicitly applicable in the cyberspace context. The current CDC quarantine program and rules are premised on a narrowly tailored approach to strike a balance between national security and fundamental rights. Notwithstanding the fact that malicious code is similar to communicable diseases in name (i.e., viruses) and analogous in how it

242. *See* Dave Aitel & Matt Tait, *Everything You Know About the Vulnerability Equities Process Is Wrong*, LAWFARE BLOG (Aug. 18, 2016), https://perma.cc/BT9J-2VP9; *cf.* Christopher Krebs, *Closing a Critical Gap in Cybersecurity*, LAWFARE (Dec.BLOG (Dec. 16, 2019), https://perma.cc/UJ5Z-V8KH (highlighting some of the gaps in the current government-run Vulnerabilities Equities Process and limits on notifying the private sector entities regarding vulnerabilities); Kate Charlet, Sasha Romanosky & Bert Thompson, *It's Time for the International Community to Get Serious about the Vulnerability Equities Process*, LAWFARE BLOG (Nov. 15, 2017), https://perma.cc/FJ89-8XG3.

243. *See generally* Control of Communicable Diseases, 82 Fed. Reg. 6890 (Jan. 19, 2017) (42 C.F.R. Pts. 70 and 71).

might spread, the federal health quarantine rule also addresses many of the same concerns that are present in the cyber context. The following paragraphs outline some of these concerns, considerations, and benefits that flow from Congress using the CDC federal quarantine rule and program as a starting template for constructing a federal cyberspace emergency authority and quarantine rule.

First and foremost, however, it would be critical for Congress to contend with explicitly addressing in a federal cyberspace emergency quarantine authority how and under what circumstances federal preemption might apply to any state or local cyberspace emergency quarantine authorities. Preemption provisions in the cyber context are particularly critical when malicious code often respects no boundaries and can spread quickly across systems and networks. In most cases of a massive cyber-attack there would likely be no time to coordinate or resolve conflicts with state or local governing bodies.

Second, Congress can use the CDC quarantine authority and program to model corresponding mechanisms that protect fundamental rights while balancing the needs of national security. A CDC federal imposed quarantine naturally involves the implications of fundamental rights similar to those in an internet shutdown, such as the First and Fourth Amendment and substantive due process concerns.[244] In order to protect the public, pursuant to the CDC quarantine rule, the federal government can issue quarantine orders that can restrict people in various ways depending on the threat.[245] A medical quarantine imposes some of the greatest restrictions on a person short of confinement. In order to then balance fundamental rights with those of national security, the CDC quarantine rule imposes multiple layers of due process rights. These include limits on the time of the quarantine, mandatory reassessments of federal quarantine orders after seventy-two hours, and appeal rights.[246] Similar temporal restrictions and due process rights could be built into a cyber quarantine or isolation program that allows for the issuance of federal orders only for well-defined and limited cyber emergencies.

In addition, the method by which the CDC quarantine program was created is important in safeguarding rights. The quarantine rule was developed through the administrative rulemaking process that engages the public, and indirectly engages world partners through non-governmental organization participation, in the

244. *See e.g.*, *id.* at 6899-6890, 6929 (addressing First, Fourth, and Fifth Amendment concerns and various exceptions, such as, the Fourth Amendment "special needs" doctrine); *see also Jacobson v. Massachusetts*, 197 U.S. 11, 25 (1905) (recognizing the power of the state to issue "quarantine laws and 'health laws of every description'"); *cf.* Marc Santora, *New Jersey Accepts Rights for People in Quarantine to End Ebola Suit*, N.Y. TIMES (July 27, 2017) https://perma.cc/4PEU-9Q87 (New Jersey quarantine rules were modified to now require extensive due process rights after Nurse challenged state quarantine rules in 2014 after Ebola exposure and subsequent quarantine.).

245. *See* Control of Communicable Diseases, 82 Fed. Reg. at 6893, 6923, 6970, 6971 (42 C.F.R. §§ 70.5-70.6).

246. *See id.* at 6900.

process.[247] The public has an opportunity through the process to comment and participate in the rulemaking process.[248] This method not only ensures that there is some public buy-in to the program—that can help with eventual acquiescence—but also allows for individual rights and concerns to be presented, evaluated, and addressed in a nonpartisan manner.

Third, any legislation Congress introduces should consider an appropriate lead agency or regulator for the program and implementation of rules. For an analogous cyber quarantine program to operate, the DHS's Cybersecurity and Infrastructure Security Agency (CISA) could serve as the lead agency or regulator for the program, similar to the CDC in the medical realm. The newly minted CISA seems best poised to take on this role given it has already started to serve as a form of cyber FEMA-like agency,[249] given its significant role in domestic incident response.[250] The CISA also has organic to it the National Cybersecurity and Communications Center (NCCIC) that has the mission of "cyber defense, incident response, and operational integration center."[251] The NCCIC is now the central hub in government cybersecurity that incorporates all of the national level emergency response legacy organizations.[252] The NCCIC's mission, rich history, and expertise in cyberspace emergency response may then make it well-positioned to serve within CISA as a type of operations center for a massive cyberspace emergency that could oversee a quarantine program, if it is ever needed.

Fourth, another aspect of the federal health CDC quarantine program that Congress should consider exporting into the cyber context is enforcement through criminal sanctions.[253] Sanctions can carry over into the cyber context to ensure the desired effects of any directed quarantine or overall program requirements. However, monetary sanctions or the threat of future restrictions on the access of certain types of data may serve as a more powerful incentive in the cyber context. For some big data companies, restrictions on data would be an extremely meaningful compliance tool. As the common adage goes, "data is money" in the big data and information age.

Fifth, the CDC generally has a mechanism under the quarantine rules and program to engage in health exams to monitor health.[254] After a massive directed cyber-attack, the government might use a similar authority to conduct a mandatory exam on either public or private systems to ensure risks have been addressed

247. *See* CENTER FOR DISEASE CONTROL AND PREVENTION, CDC REGULATIONS, CDC'S ROLE IN RULES AND REGULATIONS, https://perma.cc/UWL9-YP3P.

248. *See id.*

249. *See* Krebs, *supra* note 242 (discussing CISA's creation and service as the nation's "risk advisor").

250. *See* Dep't of Homeland Security, CISA, *Cyber Incident Response*, DHS.GOV, https://perma.cc/J7JA-4J67.

251. *See* Dep't of Homeland Security, CISA, *National Cybersecurity and Communications Integration Center*, DHS.GOV, https://perma.cc/G89D-J5FK.

252. *See id.*

253. *See* 42 U.S.C. § 271; 18 U.S.C. § 3571.

254. *See* 42 C.F.R. §§ 70.12 and 71.36.

and mitigated. Accordingly, Congress might also consider adding such an authority for cyber. Yet, taking this a step further and shifting from the narrow issue of a quarantine authority, the CDC health monitoring mechanisms can offer an even broader application in a cyber context. A facet of a cyber program could build on this idea of health exams and mandate some type of periodic cyber "health" exams for government, critical infrastructure, and the private sector. Exams might be conducted on an annual basis (like a type of audit) to identify overall risks in the system and approaches to improving the systems. For the most part, government agencies take part in similar periodic risk assessments that have now become far more robust over the last couple of years.[255] The Office of Management and Budget, in coordination with DHS, typically conduct these assessments to identify risks and offer guidance to reduce those risks, for instance.[256]

A goal for Congress might then be to extend such exams to the private sector, starting with critical infrastructure or large companies with vast infrastructures, to maintain overall cyber "health" of national cyber infrastructure. A "sickness" in one system can easily spread to other systems or create the environments for which the "sickness" can spread, without regard for whether it is government or private, firewalls sometimes notwithstanding. It is time national policy toward cybersecurity truly embodies this long-accepted understanding.

Legislation in this area, therefore, should require all private and public entities, either using their own networks or dealing with data flow across networks, to not only maintain comprehensive cybersecurity and data security programs, but also undergo periodic cyber "health" exams. Cyber "health" exams could be maintained in privilege to avoid disclosure for litigation, which is a concern for many in the private sector and a potentially a current barrier for participation with government or getting assessments. For critical infrastructure, the government may be the one administering the exam. Private entities, instead, could remain eligible to secure private examiners. Small businesses might also receive subsidies in order to obtain these exams. These are only but a few of the potential ideas for implementation.

To some extent, though, it may remain critical for certain private entities to have their cyber "health" exams be accessible to the public. For instance, this may be desirable in the case of those big data firms, financial firms, or healthcare entities that deal in sensitive personal information. It may be considered a public good to inform people about how their data is being secured and allow them more control over the choices they make in selecting how to share their information and with whom. Of course, an option would be to still keep these "health" reports inaccessible for use in litigation against private claims against businesses. Such

255. *See generally Ensuring the Cybersecurity of the Nation,* U.S. GOV'T ACCOUNTABILITY OFF., https://perma.cc/9UMJ-J22E; EXEC. OFFICE OF THE PRESIDENT, FEDERAL CYBERSECURITY RISK DETERMINATION REPORT AND ACTION PLAN (2018), https://perma.cc/XVB4-7WD3.

256. *See id*. at 3.

provisions only begin to scratch the surface of the related privacy and information sharing concerns that could similarly be addressed through such legislation; however, further discussion on these facets exceeds the scope of this paper.

Finally, and critically, Congress' implementation of legislation addressing a cyber national "health" and quarantine program may be able to change the perspective on cybersecurity today, leading to a more secure nation overall. There is a lot in a name; messaging and labels can matter. A program aimed at maintaining the "health" of cyberspace rather than the "security" may engender more public support and acceptance. A program aimed at "health" shifts the focus to something the everyday person can appreciate, whereas securing networks for national security may not be something the general public can grasp or is incentivized to protect, largely due to much of the secrecy shrouding this sector. Eventually, the program will still work to that end while also addressing the rare case that government may need the authority to exercise a cyber quarantine, isolation, or shutdown of the internet or networks within the United States.

CONCLUSION

Congress has not left the authority to quarantine, isolate, or shutdown computers or portions of the internet or networks in a time of emergency an "open field."[257] These authorities most certainty do not lie with the Executive, as confirmed by the above analysis of presumed Executive and emergency authorities in cyberspace. Instead, this article concludes that Congress most certainly left it an uncertain field.

Current legal authorities in the United States are inadequate to address the possible need for a government-imposed internet shutdown to defend against, recover, and maintain resilient networks during and after a cyber-attack. More realistically, though, in practice this comes in the form of targeted shutdowns of computers or portions of the internet or networks to slow or stop the spread of malicious attacks, issue anti-virus batch files or patches, or take vulnerable or targeted computers or networks off the internet.

Consequently, legislation is required to clarify legal authorities that would allow for such measures and to set up an appropriate framework that can go beyond protecting only government and critical infrastructure systems. Modern interconnectedness demands a comprehensive national cyber response framework that also addresses the private sector and individuals, while maintaining respect for civil liberties. A national cyber "health" and quarantine program may be the first step in accomplishing that goal and protecting the nation.

A healthy cyber nation focused on cyber "health" instead of security is a potential way to change the discourse surrounding cybersecurity today. This may be

257. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 587, 639 (1952) (Jackson, J., concurring).

the key to awakening the public to the real concerns surrounding cybersecurity and the vital role they play in securing the nation. It also makes sense in light of the growing acceptance that "digital" or "cyber" is now an inextricable part of Americans' everyday lives. In the end, overall increased cybersecurity compliance and wide-spread participation is the only means toward ultimately improving national security in cyberspace, and hopefully can result in never having to build cyber walls in the first place.

***