Hastings Constitutional Law Quarterly

Volume 50 | Number 4 Article 3

5-2023

Preserving Constitutional Integrity in the Age of Cyberwarfare: A Paper Tiger, or Death by a Thousand Cuts?

Darren Singh

Preserving Constitutional Integrity in the Age of Cyberwarfare: A Paper Tiger, or Death by a Thousand Cuts?

BY DARREN SINGH*

Abstract

The Constitution is meant to serve as a necessary constraint on unilateral Executive military actions. Today, nation-states and non-state actors can launch devastating cyberattacks on the infrastructure, economy, military, and democratic systems of the United States. These attacks do not fall within the realm of "hostile actions" necessary to constitute war. Cyberattacks from adversaries are best deterred with offensive cyberattacks of our own. The President is the best actor to superintend and direct this active defense. Neither the Constitution nor the War Powers Resolution, however, offer a framework for how the United States may respond to these threats while also balancing shared war powers. Congress should prevent the further expansion of precedence granting the Executive access to an entire destructive technology alone and without accountability.

* Captain Darren Singh is a J.D. Candidate 2023, University of California Hastings College of the Law; B.A. 2016, San Francisco State University, English. I am grateful for the support of my friends and family throughout the process of writing this Note. I owe great thanks to Professor Coles and Professor Rappaport for their guidance. I am also grateful for my many mentors and peers in uniform who have inspired me to continue a life of service through our shared time in the Army. And finally, a special thanks as well to the editors of CLQ for their help bringing this Note to fruition. The views expressed here are the authors alone. They do not reflect the official position of the U.S. Army or any of its subordinate units, the Department of Defense, or the United States Government. Any and all errors are my own.

TABLE OF CONTENTS

Introduction

In 2010, the Iranian government aggressively pursued a uranium-enrichment program that many believed was primarily poised to help the renegade nation achieve its goals of nuclear armament.[1] Diplomacy had stagnated into a logjam. Conventional military action seemed a disastrous, ill-fitting, and disproportionate response, when suddenly, Iran suffered a deep set-back. It was not the result of artillery bombardments, precision airstrikes, or conventional espionage. It was the result of the most sophisticated malware yet seen: the Stuxnet worm.[2] The worm is widely believed to have been inserted into adjacent computer systems via USB hard drive to defeat air gap[3] defenses.[4] For months, the virus promiscuously infected multiple computer platforms at the Natanz nuclear site. Like a laser-guided cancer, the worm exclusively commandeered the industrial control systems on which nuclear centrifuges operated. It then forced the programs to behave in ways that caused irreparable damage to the host centrifuges, all while avoiding detection.[5] Stuxnet caused the centrifuges to effectively self-destruct, and the setback likely delayed Iranian advances in their pursuit of a nuclear weapons program.[6]

Since Stuxnet, the world has not viewed cyberwarfare or cyberterrorism the same. A decade ago, the United States had already begun to view cyberwarfare as the cutting edge of battlespace.[7] However, post-Stuxnet, U.S. fears were aligned around imagining disastrous, single-incident strikes that could take lives, damage infrastructure, and cripple conventional warfighting functions akin to Weapons-of-Mass-Destruction (WMDs).[8] These fears centered around a hypothetical "cyber-Pearl Harbor" in which then-Secretary of Defense Leon Panetta warned of possible cyberattacks that could potentially shut down entire power grids or crash financial systems. In large part, these warnings were meant to serve as a clarion call for the

1. Greg Bruno, *Iran's Nuclear Program*, COUNCIL ON FOREIGN REL. (Mar. 10, 2010, 7:00 AM), https://www.cfr.org/backgrounder/irans-nuclear-program.

2. PAUL K. KERR ET AL, CONG. RSCH. SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY (2010).

3. Air gapping is a security measure wherein a computer or network is isolated from other computers or networks. A specified amount of space is allotted between a system and outsides walls and wires–like a moat.

4. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

5. *Id.*

6. Kerr, *supra*, note 2.

7. Sue Gordon & Eric Rosenbach, *America's Cyber Reckoning*, FOREIGN AFF. (Dec. 14, 2021), https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning.

8. *Id.*

American public to galvanize around supporting the government's recent deeper investment in a still nascent U.S. cyber-defense apparatus—evidenced by the then recently formed, U.S. Cyber Command.[9] However, when a catastrophic digital disaster did not come to pass, many derided cyberwarfare and cyberterrorism threats as more akin to vandalism than a legitimate means of war—a paper tiger more imposing in its appearance than its bite.[10] Geopolitical rivals of the United States in the last few years have quickly disproved this assessment, as cyberwarfare has been used more and more aggressively against the United States.

The Stuxnet operation was not exactly the imagined and dreaded "cyber-Pearl Harbor" that Leon Panetta may have had in mind, yet it was not mere vandalism either. Cyberwarfare has become a more complicated and crowded battlespace—with operations ranging from simple distributed denial-of-service (DDoS) attacks to destructive attacks on infrastructure. Cyberwarfare has been used not only to chip away at digital and real infrastructure but even more often to sow distrust within a society, damage economic systems, and steal information vital to a nation's interest. It may seem a paper tiger, but unchecked, thousands upon thousands of small cuts against U.S. power will begin to inflict serious damage. This Note hopes to offer a solution to filling in the gap.

While many geopolitical rivals use these types of attacks against the United States with impunity, the United States must navigate constitutional issues before choosing how to respond. When an adversary tears down the internet in part of the country, it remains unclear if this is an attack on the nation. If it is not, the issue of whether the President may respond, and in what manner, remains a similarly unresolved legal standard. The role Congress may play in this hypothetical situation remains far too passive, complicated by the political realities that must similarly be resolved. This Note seeks to reach a policy framework by which the President has the tools they need to deter adversarial cyberwarfare, and wherein Congress does not doctrinally cede to the Executive's unilateral access to offensive cyberwarfare actions. Congress simply ceding to the Executive could and would make the balance of power between the branches even more lopsided than status quo ante, which could set up the branches for constitutional conflict.

Part I seeks to provide the factual and legal context in which cyberwarfare has emerged as the cutting edge of battlespace, detailing the

9. Adam Stone, *How Leon Panetta's 'Cyber Pearl Harbor' warning shaped Cyber Command*, FIFTH DOMAIN (July 30, 2019), https://www.fifthdomain.com/opinion/2019/07/30/how-leon-panettas-cyber-pearl-harbor-warning-shaped-cyber-command/.

10. Ben Buchanan, *Five myths about cyberwar*, WASH. POST (Feb. 20, 2020), https://www.washingtonpost.com/outlook/five-myths/five-myths-about-cyberwar/2020/02/20/54d89458-5289-11ea-b119-4faabac6674f_story.html.

unique challenges associated with this space. Part II will outline why a lack of a legal framework that is tied to the actual realities in the real world is a structural weakness that our adversaries can exploit. Part III will offer a solution based on legal precedent, while also offering new ideas for creating a scheme that still maintains constitutional integrity. Part IV will address counterarguments and potentially difficult areas in the proposed framework's implementation.

While this Note will broach the broad subject of cyberwarfare, it will *not* analyze in-depth cybercrime or "hacktivism." This Note will instead focus on direct action cyberwarfare from the foreign state and non-state actors. It will not focus on domestic actors internal to the United States. Finally, this Note will focus on these aspects from a constitutional law lens, rather than an international law lens.

I. Background: Cyberwarfare & Executive Power

"Cyberattack" is a relatively recent term and can refer to a range of activities. For example, one of the most popular, and easily implemented types of cyberattack is a DDoS attack.[11] DDoS attacks work to disrupt network traffic for a targeted server to effectively cut off internet access.[12] However, like the Stuxnet cyberattack proves, cyberattacks can do more than simply shut down internet services, like DDoS attacks. In some of the most sophisticated cases, cyberattacks can trick systems and sabotage large databases or mechanical processes. In 2012, Harold Koh imagined possible worst-case scenarios, such as using cyberattacks to electronically open a dam to cause flood damage or causing airplanes to crash through deliberate interference with air traffic control.[13]

Beyond disruption, disinformation, and sabotage, cyberattacks have been most effective at producing economic damage or illicit economic gains. For example, the American economy has lost $200 billion to $600 billion dollars a year in intellectual property to Chinese hackers[14] The United States has no effective response to these large windfalls because these are clearly not 'traditional' attacks against the United States. Ransomware, a type of virus, has been another medium that blends the line between cybercrime and cyberattacks. Ransomware threatens to lock systems or to destroy data systems if the user does not pay money to the extorter–and in 2017 it was used to great effect against the British National Health Service; similarly, it was

11. CATHERINE A. THEOHARY & JOHN W. ROLLINS, CONG. RSCH. SERV., R43955, CYBERWARFARE AND CYBERTERRORISM: IN BRIEF (2015).

12. *Id.*

13. *Id.*

14. Joseph S. Nye, Jr., *The End of Cyber-Anarchy?*, FOREIGN AFF. (Dec. 14, 2021), https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

also later an issue during the COVID-19 pandemic as well.[15] Ransomware can go beyond being purely economic. It may be used to lock up election software during American elections, in exchange for exorbitant amounts of money.[16] A loss in confidence in American elections due to malfunctioning systems would be of great strategic value to adversaries and directly degrades U.S national power. Can this be defined as an act of war? It is into the extremely diverse set of circumstances and threat actors that one tangles with when developing a statutory legal framework that is flexible enough to respond decisively to all situations and all threat actors.

A. The History and Range of Cyberwarfare: The United States is Beleaguered by a Diverse Range of Cyberthreats & Cyberactors

Around the same time Stuxnet was discovered, the United States formed Cyber Command. When it was first formed in 2010, and throughout its first 6 years, the United States took the position that U.S. Cyber Command would not take part in assertive information [cyber] warfare itself.[17] This mentality reflected the fear that cyberwarfare may lead to a classic escalation into traditional kinetic warfare. This reticence led to only passive defenses being implemented.[18] Later, U.S. Cyber Command learned that offensive cyberoperations were also the best defensive operations.

Prior to Stuxnet, cyberattacks primarily consisted of simpler DDoS attacks, such as the suspected Russian cyberattacks on Estonia that later gave rise to the creation of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) in Estonia, and then the creation of the Tallinn Manual.[19] The Tallin Manual was primarily an international law document, more academic than authoritative.[20] As a sort of template for black letter rules on cyberwarfare between nations, the Tallinn manual remained mostly a "rule book left on the shelf," with most nations demonstrating a reluctance to accept the Tallinn Rules, and an uneven interest in even legally regulating cyberspace.[21] Thus, for most, Stuxnet opened Pandora's box to the full potential of cyberwarfare, kickstarting a new era of warfare.

---

15. *Id.*

16. THE PERFECT WEAPON (HBO Documentary Films 2020) at 81:00.

17. Gordon & Rosenbach, *supra*, note 7.

18. *Id.*

19. *Id.* at 4; MAJ William C. Ashmore, United States Army Command and General Staff College, *Impact of Alleged Russian Cyber Attacks* (2009), at 9, https://apps.dtic.mil/sti/citations/ADA504991.

20. Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights,* 48 GEO. J. INT'L L., 735 (2016).

21. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice,* 112:4 AM. J. INT'L LAW. 583 (2018).

In August 2012, a series of cyberattacks were levied against Saudi Aramco, the world's largest oil and gas producer.[22] The attacks compromised over 30,000 systems and were designed to disrupt or even halt oil production. The repercussions this could have on national security and the global economy cannot be understated. While some cybersecurity and intelligence officials believe Iran could have been partially responsible—problems of attribution make it difficult to lay blame, thus making it difficult to lay legal and political accountability.[23] Only two years later, in 2014, Sony Pictures was about to release the movie "The Interview."[24] North Korea put the newly minted, but slow and cumbersome, U.S. cybersecurity apparatus to the test when it conducted the first ever destructive cyberattack on U.S. soil in the Sony Pictures cyberattack.[25] Sony lost tens of millions of dollars in the attack and a large trove of sensitive data was stolen from them.[26]

In 2015, the United States Office of Personnel Management announced that it had been breached in a cyberattack all throughout the last year, which led to the greatest theft of sensitive personnel data in history.[27] The data included sensitive, personal, and discrete details of thousands of Americans who work throughout the government and hold security clearances.[28] The overwhelming consensus in the cybersecurity and intelligence communities came to believe that Chinese-state-backed actors had perpetrated the hack—the impact was enough to lead to the Central Intelligence Agency canceling assignments for operatives who were originally going to be working undercover in China, or adjacent.[29]

In 2018, Russian government hackers began to target energy systems in the United States, executing a cyberoperation to scout and collect information on energy generation within the country.[30] U.S. officials began to fear this was in large part for Russian cyberwarfare experts to determine if

22. Gordon & Rosenbach, *supra*, note 7.

23. *Id.*

24. *Id.* (The Interview is a fictitious, comedy film in which Seth Rogan and James Franco attempt to assassinate Kim Jong-un.).

25. Gordon & Rosenbach, *supra*, note 7.

26. THE PERFECT WEAPON (HBO Documentary Films 2020) at 27:00 .

27. Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE BLOG (Mar. 11, 2016, 10:00 AM), https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

28. *Id.*

29. John Fruhlinger, *The OPM hack explained: Bad security practices meet China's Captain America*, CSO (Feb. 12, 2020, 5:15AM), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

30. Cybersecurity & Infrastructure Sec. Agency, *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (Mar. 16, 2018), https://www.cisa.gov/uscert/ncas/alerts/TA18-074A; Kelsey Atherton, *It's not just elections: Russia hacked the US electric grid*, VOX (May 28, 2018, 8:00 AM), https://www.vox.com/world/2018/3/28/17170612/russia-hacking-us-power-grid-nuclear-plants.

and how they could shut down the U.S. power grid at some later date.[31] This should illustrate that the range and threat of cyberoperations is wide and still growing.

Today, the United States possesses a Cyber Command that was promoted to its own combatant command status as of 2018.[32] United States Cyber Command is now one of the eleven unified combatant commands of the United States Department of Defense. This freed Cyber Command from being subordinately aligned under a slow-moving Strategic Command, and now reflects a faster, more fluid and flexible disposition from which to respond assertively to cyberattacks. Now, the U.S. military makes a more robust and serious assessment of cyberthreats, and classifies cyberspace as the "fifth domain" of warfighting, no different than fighting on land or sea; acknowledging that effects from cyberwarfare can bleed into other domains.[33] Maybe mirroring this unshackling organizationally, since 2011 the executive branch's legal stance has also become increasingly unshackled from passivity, evidenced in the Obama-era promulgation of the 2011 International Strategy for Cyberspace. This document broadly asserted executive authority to respond to cyberattacks by *any* means appropriate as self-defense right.[34] This was a very significant stepping-stone that made clear that the Executive branch was willing to respond to adversarial or hostile cyberoperations with whatever tools are available to the United States, including more traditional, kinetic military responses as well as diplomatic, or economic levers of power.[35]

In response to the 2018 Russian cyberattacks on the U.S. electrical grid, the United States Cyber Command incorporated more aggressive tactics, launching multiple cyberoperations against Russia in order to meet and match the hostile Russian probes into the U.S. electrical grid.[36] U.S. Cyber Command successfully infiltrated Russia's electrical grids, signaling in clear and non-covert messages that Americans were present in the system.[37] Contemporaneously, the U.S. launched several cyberoperations to identify and message multiple Russian-backed hackers, clearly warning them of

31. *Id.*

32. Gordon & Rosenbach, *supra*, note 7.

33. NAT'L SEC. LAW DEP'T., U.S Army Judge Advocate General's Legal Center School, *Operational Law Handbook* (2021), https://tjaglcs.army.mil/publications [hereinafter Op Law Handbook].

34. EXEC. OFF. OF THE PRESIDENT, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 16, 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.

35. *Id.*

36. THE PERFECT WEAPON (HBO Documentary Films 2020) at 66:16.

37. *Id.*

repercussions in the case of any election tampering.[38] The strategy was met with success, and throughout Russia, cyberactors remained relatively quiet for the rest of 2018.[39] U.S. Cyber Command had proved that, while not a permanent solution, offensive cyberoperations could successfully deter cyberactors. Where passive defenses require meeting the impossible task of building a perfect defensive system and constantly catching new threats, an offensive cyberoperations program served as a much more effective deterrent.[40]

However, even if the U.S.'s strategic resources and overall tactical understanding of the cyberthreat has grown exponentially alongside and parallel to the increasing complexity of foreign threats, a compatible legal framework has failed to grow alongside this military capability. The Tallin Manual mostly nested itself as an international law document that served as a general guideline. There has not and is not any real consensus between the legislature and executive on offensive cyberwarfare as they pertain to the War Powers debate, or on the President's authority to launch offensive cyberwarfare operations.

In the absence of guidance, or any real restrictions, President Trump delegated his authority to launch cyber-attacks down to then-Cyber Command Commander, General Nakasone. The general's success with the Russia Small Group, the U.S. force that successfully countered Russian hackers in 2018 begged the question: was this the new norm?[41] It was then unclear if this discretion was the President's alone. Traditionally, where Congress does not clearly assert itself, the Executive branch is invited to act of its own accord.

B. The War Powers in Perennial "Twilight:" The Shared Powers Debate

The long debate on the War Powers Resolution is not new. Under the U.S. Constitution, the President shares war powers with Congress and vice versa. The bifurcated nature of the war powers was intended. Under Article II, Section 2 the President derives their war powers as the named Commander-in-Chief.[42] Furthermore, the President derives power from the Take Care Clause, as well as the Reception Clause.[43] As the Commander-in-Chief, the President has broad authority under Article II, but also on all foreign affairs matters, and this is a fairly noncontroversial viewpoint.

38. *Id.*

39. *Id.*

40. Dmitri Alperovitch, *The Case for Cyber-Realism*, FOREIGN AFF. (Dec. 14, 2021), https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism.

41. Gordon, *supra*, note 7, at 5.

42. U.S. CONST. art. 2, § 2, cl. 1.

43. U.S. CONST. art. 2, § 3, cl. 1.

Deference to the Executive in aspects of foreign affairs is fairly commonplace in the many precedents on the topic.

The United States Congress has significant authority in war and military matters as well. Under Article I, Section 8, only Congress has the ability to declare war and fund the military.[44] Congress is to promulgate rules and regulations for the military.[45] Further, advocates for more Congressional involvement also argue that the Necessary and Proper Clause further reinforces the powers of Congress in this realm too.[46]

Adding to this baseline understanding, Justice Jackson's famous 1952 concurrence in *Youngstown Sheet & Tube Co. v. Sawyer* offers an informative framework for understanding the operation of the shared powers between the Commander-in-Chief and Congress.[47] Justice Jackson famously laid out three zones: (1) where Congress has expressly or impliedly granted power to the Executive, the President may rely upon their own powers and those of Congress, and here they *personify* the federal sovereignty;[48] (2) where Congress remains silent, the President may rely only on their own [inherent] authority, but there is a zone of twilight in which they and Congress may have concurrent authority, but Congressional indifference or acquiescence invites the President to act independently; and (3) where the President acts contrary to the will of Congress, their power is at its lowest ebb.[49]

Beyond the Supreme Court's classic formulation, in the aftermath of the Vietnam War, Congress passed the War Powers Resolution ("WPR")[50] as a joint resolution. It was an immediate response to presidential power to commit troops abroad without Congressional consent and meant to create a statutory safeguard of Congressional participation in war. The WPR was designed as a means to ensure that legislature would be more proactively involved whenever United States Armed Forces (U.S. Forces) were introduced into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances.[51] The most important aspects of the WPR craft a clear procedure for how the Executive branch is encouraged to engage with the Legislature. Under section 1542, the President is encouraged to consult with Congress *before* introducing U.S. Armed

44. U.S. CONST. art. 1, § 8, cl. 1 & 11.

45. U.S. CONST. art. 1, § 8, cl. 14.

46. David J. Barron & Martin S. Lederman, *The Commander in Chief at Lowest Ebb*, 121:68, HARV. L. REV. 691, 735 (2008) (discussing how Necessary and Proper Clause reinforces Congress' shared war powers).

47. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

48. *Id.* at 635–36.

49. *Id.* at 637.

50. 50 U.S.C § 1541–50.

51. 50 U.S.C § 1541(a).

Forces into hostilities or into situations with imminent involvement in hostilities.[52] Under section 1543, the President is required to comply with reporting requirements, including legal justifications for the introduction of U.S. forces and the estimated scope and duration of the involvement.[53]

One of the most significant functions of the WPR is codified in section 1544, which starts the infamous "60-day" clock after U.S. Armed Forces are committed (ostensibly after an initial section 1543 report is filed).[54] The WPR demands that the President terminate use of the U.S. Armed Forces after the 60-days unless (1) Congress has declared war or enacted an Authorization for such use, (2) extended by law the 60-day period, or (3) is physically unable to meet as a result of an armed attack upon the United States.[55] Section 1544 further lays out a procedure by which, notwithstanding the 60-day period, at any time, Congress may pass a concurrent resolution that requires the President to recall U.S. forces.[56]

However, the WPR has largely been ineffective throughout the decades since its passing.[57] Congress has not enforced the WPR against any President persuasively, even for actions amounting to far greater use of force than the majority of cyberoperations may constitute.[58] The WPR has been the source of very animated debate within legal scholasticism, and many proposed solutions have been offered to retool, or revise the WPR to arm it with "teeth," even as so recently as the last few years during the on-going War on Terror.[59] Today, as of this writing, it remains the central bridge between Congress and the President on the issue—even if it is a bridge broken and rarely crossed.

C. Authority to Use Military Force: Executive Precedent under Bush and Obama

Declarations of war are rare. After the September 11th terror attacks, President Bush relied upon Authorizations for Military Force ("AUMF") to

52. 50 U.S.C § 1542 (emphasis added).

53. 50 U.S.C § 1543.

54. 50 U.S.C § 1544(b).

55. *Id.*

56. 50 U.S.C § 1544©.

57. John Hart Ely, *Suppose Congress Wanted a War Powers Act that Worked*, 88, COLUM. L.R. 1379 (1988) (discussing that the War Powers Act has proven unworkable due to a history of Executive non-compliance and how Congress has not, or cannot 'call him on it.').

58. Brian J. Litwak, *Putting Constitutional Teeth into a Paper Tiger: How to Fix the War Powers Resolution*, 2:2, AM. UNIV. NAT'L SEC. L.B. 1, 5-10 (2012) (asserting that judicial reluctance to enforce the WPR plus congressional inability has led to the WPR becoming a 'byzantine legal edifice.').

59. Kyle C. Walker, *Operation Inherent Resolve and the Reemergence of the Debate over the War Powers Resolution*, 43, HASTINGS CONST. L.Q. 423 (2016).

acquire Congressional consent to his subsequent military actions.[60] Two AUMF's were eventually issued, one pertaining to the war in Iraq and one pertaining to the broader War on Terror.[61] AUMF Iraq is in the process of being repealed, as of this writing.[62] AUMF Terror remains law and will be revisited later in this Note as a potential structural analogy for a statutory cyber-defense solution. Given that the WPR has failed to serve as a statutory tool, the Executive branches' arguments on its Constitutional stature on the shared war powers takes a central role. Before considering what a new, better statutory bridge between Congress and the President on offensive use of cyberoperations might look like, one must consider the state of the President's view of his inherent powers, as a Constitutional matter.

President Obama's presidency covered a large part of the time wherein cyberwarfare began to truly be considered a rather weighty threat. It was under his tenure that Stuxnet occurred, that U.S. Cyber Command was formed, the 2011 International Cyberspace Strategy was released, and more importantly, also when the Arab Spring occurred.[63] While the latter does not seem related to the former, they form a vitally important context. The Arab Spring was linked to a humanitarian and military crisis in Libya, eventually leading President Obama to authorize military force in the form of directed aerial strikes in order to strategically disable the Libyan military.[64] Then-Libyan leader Muammar al-Qaddafi had ordered his military to commence heavy kinetic bombing operations against cities as Libyan people began revolting against his regime.[65] The situation in Libya should not be understated: Qaddafi's forces were instructed to "show no mercy" to prisoners, and reports indicated that Qaddafi's forces were using rape as a tool of war in addition to bombings and firing of live weapons.[66] The Executive branch released its legal rationales in an Office of Legal Counsel ("OLC") opinion that found the President had the authority to constitutionally use military

60. JENNIFER K. ELSEA & MATTHEW C. WEED, CONG. RSCH. SERV., RL31133, DECLARATIONS OF WAR AND AUTHORIZATIONS FOR THE USE OF MILITARY FORCE: HISTORICAL BACKGROUND AND LEGAL IMPLICATIONS (2014).

61. *Id.*

62. Claudia Grisales, *In Historic, Bipartisan Move, House Votes To Repeal 2002 Iraq War Powers Resolution*, NPR (June 17, 2021), https://www.npr.org/2021/06/17/1007363054/congress-is-poised-to-take-back-some-of-its-war-powers-from-the-president.

63. The Editors of Encyclopedia Britannica, *Arab Spring*, BRITANNICA, https://www.britannica.com/event/Arab-Spring (last updated Jan. 27, 2021).

64. The Editors of Encyclopedia Britannica, *Libya Revolt of 2011*, BRITANNICA, https://www.britannica.com/event/Libya-Revolt-of-2011 (last updated Feb. 8, 2023).

65. *Id.*

66. Harold H. Koh, *The War Powers and Humanitarian Intervention*, 53 HOUS. L. REV. (2016).

force in Libya (OLC-Libya).[67] This OLC opinion codifies and reflects the current state of the law on shared powers, the President's ability to circumvent the WPR, and to rely on his Constitutional inherent powers arguments.

The OLC-Libya opinion found that because President Obama's deployment of military assets was in such a limited capacity, the President had constitutional authority to act within his Commander-in-Chief powers and his foreign affairs powers, with the limited airstrikes and military support functioning as a diplomatic action, that did not require prior consultation or authorization from Congress.[68]

OLC-Libya further elaborates that the President holds the "implicit advantage" over the legislature in the overall constitutional scheme in situations calling for immediate action, given that imminent national security threats require a swift, decisive response.[69] OLC-Libya further observed that there was a long history of presidential initiatives such as: bombing in Libya (1986), an intervention in Panama (1989), troop deployments in Somalia (1992), Bosnia (1995), and Haiti (twice, 1994 and 2004) air patrols and airstrikes in Bosnia (1993-1995), and a bombing campaign in Yugoslavia (1999), each without specific prior authorizing legislation.[70]

OLC-Libya's most important section, however, lays out a litmus test for determining whether a planned engagement constitutes a "war" constitutionally. OLC-Libya determines that this is a fact-specific test based on the "*anticipated nature, scope, and duration*" of the planned military operation.[71] It finds that this test will likely only be met by prolonged and substantial military deployments, inferring that oftentimes means boots on the ground.[72] Even so, if a planned deployment of 20,000 U.S. troops to Haiti in 1994 (to oust military leaders and reinstall Haiti's legitimate government) was not considered an act of war, then neither could precision airstrikes.[73] OLC-Libya referenced further incidents to buttress its analysis as well.[74]

OLC-Libya concludes with a general formula: where the President is serving sufficient important national interests and is limiting deployment of armed forces by anticipating its nature, scope, and duration, the President

67. Caroline D. Krass, *Authority to Use Military Force in Libya*, 35 OP. OFF. LEGAL COUNSEL 20 (2011).

68. *Id.* at 27.

69. *Id.* at 28.

70. *Id.* at 29.

71. *Id.* at 31 (emphasis added).

72. *Id.*

73. Walter Dellinger, *Deployment of United States Armed Forces into Haiti*, 18 OP. O.L.C. at 179 (1994).

74. Krass, *supra*, note 67, at 32.

may act without congressional pre-authorization.[75] OLC-Libya also draws a clear divide between the weightiness of troops on the ground and limited airstrikes or imposing U.S. airpower in no-fly zone patrols.[76] This opinion defined what is constitutionally "short of war," and remains an unchallenged interpretation that includes a rather robust range of actions.

II. Neither The Constitution, Nor Congress, Nor The War Powers Act Currently Provide A Clear Constitutional Path To Combat Cyberthreats

When the Framers first drafted the Constitution, it is unlikely that, even in their wildest imaginations they envisioned a world wherein entire nation-states could be plunged into darkness or left without communication systems by the actions of a handful of actors. The Constitution's division of war powers relies on a conventional understanding of war, better defined as kinetic[77] military operations.[78] The WPR does little to clarify how and if at all it would affect cyberoperations if used offensively by the U.S. or how the WPR would constitutionally classify cyberattacks from other actors. The increasing fervor, severity, and frequency of cyberattacks require the U.S. to begin implementing solutions now. Strategically, problems of attribution and asymmetry mean that adversaries require very little material investments in comparison to the disproportionate impacts against the United States and its allies, and these attacks will oftentimes be anonymous. This set of circumstances demonstrates the need for a constitutional scheme that includes a strong deterrence element made up in part with offensive U.S. cyberwarfare operations.

If the United States continues to wait before implementing a clear cyber-defense policy, adversaries and geopolitical rivals will continue to leverage cyberweapons of war against the United States. Without statutory safeguards, Congressional participation, or judicial enforcement, the Executive will continue to carve out an entire class of weapons of war for

75. *Id.* at 37.

76. *Id.* at 32, 38 (describing how for more than two years prior to the Bosnian deployment, the U.S. had undertaken air operations over Bosnia to enforce a UNSC "no-fly zone" which led to flying over 2300 sorties and also referencing aerial bombing campaigns in Kosovo, both based on the President's constitutional authority nested in foreign relations and Commander-in-Chief powers and without specific prior approval from Congress).

77. Jordan Stern, *Civil Military Operations & Military Information Support Operations Coordination: A Non-Kinetic Ballast for Disciplined Counterinsurgency Operations*, https://apps.dtic.mil/sti/pdfs/ADA552673.pdf (last updated Nov. 2011).

78. Kinetic military force, or operations are defined as the targeted application of lethal, kinetic force upon opposing forces and may be better understood as an alternate term for traditional, conventional armed force. It refers to the fact that traditional munitions rely on kinetic or physical force to destroy targets.

unchallenged use under a single branch of government. This will create constitutional conflict between branches to a degree that cannot possibly be predicted or mitigated against.

A. Problems of Attribution: When Adversaries are Unknown, All Actors Must Understand the United States Possesses a Robust Cyber-Defense & Clear Cyber-Policy

Cyberattacks are unique from traditional forms of espionage or adverse kinetic operations because they are difficult to detect, track and attribute to a specific actor.[79] When a nation fires a missile, typically it is very clear that the weapon will be attributed to its host nation because a missile cannot simply be hidden. This serves as a significant socio-political deterrent. A missile-strike from one nation state to the other will almost assuredly be classified as a use of force.[80] It could be considered an initiation of hostilities, and in some instances, it can certainly be seen as an act of war.[81] When the Saudi-Aramco attacks occurred, recall that while there was some substantial evidence or belief that Iran may be behind the attacks, there was not enough to hold the nation accountable.[82] Like state-sponsored terrorism, this may also be because many nation-states may contract or back channel with practiced cyberactors to further inoculate themselves from political accountability.[83]

A frequent lack of attribution means that opportunities for the President to respond to cyberattacks will be far and few in-between and that the best form of deterrence may actually be a robust offensive cyberoperations apparatus that will deter unknown actors from pursuing cyberattacks against the United States. A further investment in cyber-defense technologies can enable the U.S. cyber-defense apparatus to identify perpetrators of these attacks. Even as U.S. Cyber Command has risen to this challenge in the last few years, there remains a lack of constitutional consensus and collaboration between government branches, leaving difficult decisions around offensive cyberoperations to the executive branch alone.

---

79. Johann-Christoph Woltag, *Cyber Warfare*, (Intersentia, 2014).

80. JUSTIA, *Use of Force Under International Law*, https://www.justia.com/international-law/use-of-force-under-international-law (last reviewed June 2021).

81. Joseph R. Biden Jr., *Remarks by President Biden on Russia's Unprovoked and Unjustified Attack on Ukraine*, THE WHITE HOUSE (Feb. 24, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/02/24.

82. Gordon, *supra*, note 7.

83. Peter Suciu, *Everyone is Hacking These Days,* CLEARANCEJOBS (Feb. 24, 2022), https://news.clearancejobs.com/2022/02/24/u-s-has-cyber-enemies-more-than-the-usual-list-with-offensive-hacking-in-the-mix.

B. Problems of Asymmetry: When Adversaries Can Attack Asymmetrically, the United States Must Institute a Procedure that Enables Deterrence Sooner Rather than Later

An even larger and more troubling aspect of cyberwarfare is the asymmetrical nature of the medium. Asymmetrical warfare allows smaller, less traditionally powerful actors to affect larger, more powerful entities.[84] The U.S. has few peer or near-peer threats in traditional military strength.[85] However, this has invited adversaries to utilize asymmetric warfare, since it allows conventionally less powerful groups to enact effects upon us. Terrorism and guerilla warfare are examples of asymmetrical warfare, and both have been used to great effect against the United States.[86]

Cyberwarfare will continue the trend of asymmetric warfare, but even more troubling than terrorism or guerilla warfare, cyberwarfare can be, and mostly is, conducted remotely. There are a multitude of examples: such as the DPRK-Sony hack in which a nation where only 10% of its population have access to a cellphone was able to hack into a major U.S. corporation.[87] Alternatively, consider how a single individual was able to shut down an entire country's internet.[88] As of this writing, Russia is in the midst of an invasion of the sovereign nation of Ukraine.[89] Among those responding to Russia are the hacking collective, Anonymous, which is privately launching its own cyberattacks against the Russian Federation, taking down multiple Russian websites and causing communications disruptions.[90]

In cyberspace, attackers have an inherent advantage in that the relative time and value cost of each attempted hack is low, and the penalties almost nonexistent.[91] Thus, hackers seeking to infiltrate even hardened targets can

84. Ellen Sexton, *Asymmetrical Warfare*, BRITANNICA, https://www.britannica.com/topic/asymmetrical-warfare (last updated Nov. 17, 2016).

85. LOWY INST., *Lowy Institute Asia Power Index 2021 Edition*, https://power.lowyinstitute.org/data/military-capability (last visited Mar. 3, 2022); GLOB. FIREPOWER, *Military Strength Comparisons for 2022*, https://www.globalfirepower.com/countries-listing.php (last visited Mar. 3, 2022).

86. *See* Charles T. Cleveland, *The American Way of Irregular War*, 9 (RAND Corporation, 2020).

87. THE PERFECT WEAPON (HBO Documentary Films 2020) at 34:00.

88. Andy Greenberg, *North Korea Hacked Him. So He Took Down Its Internet*, WIRED (Feb. 2, 2022, 11:43 AM), https://www.wired.com/story/north-korea-hacker-internet-outage.

89. Paul Kirby, *Why is Russia invading Ukraine and what does Putin want?*, BBC (Feb. 24, 2022), https://www.bbc.com/news/world-europe-56720589.

90. James Purtill, *Hacker collective Anonymous declares 'cyber war' against Russia disables state news website*, ABC SCIENCE (Feb. 24, 2022, 11:27 PM), https://www.abc.net.au/news/science/2022-02-25/hacker-collective-anonymous-declares-cyber-war-against-russia/100861160.

91. Dmitri Alperovitch, *The Case for Cyber-Realism*, FOREIGN AFFAIRS, Jan./Feb. 2022, at 47.

afford to spend a large amount of time trying to find a way into a system to wreak havoc.[92] On the offensive, you only need to get lucky once, whereas defenders must detect and stop each and every hacking attempt.[93]

The strength of asymmetry combined with anonymity means one thing: passive defenses are not enough. This is a lesson that the U.S. military has already learned, reflected in the realignment of U.S. Cyber Command, and the more offensive response options exercised by General Nakasone in 2018. The 2018 retaliatory responses' success against Russian actors, one of the most advanced cyberwarfare nations today, vindicates this theory.

However, where U.S. military force is involved the Constitution first controls. A working legal framework, informed by both political branches must guide the military, not the other way around.

C. Problems of Presidential Power: Congress Must Limit Presidential Power

Today, as far as the Constitution and cyberwarfare are concerned, American leadership sits in a perennial Jacksonian twilight. If an offensive cyberwarfare program is one of the better solutions to deter adversarial cyberwarfare, the President and the military must first fulfill a few threshold questions. Namely, whether the use of cyberattacks against foreign adversaries constitutes hostilities that require a prior consultation with Congress, pursuant to WPR section 1542. This question has not been clearly addressed, and there have been very few challenges from the Courts or Congress that have produced the precedent to help answer this question.

OLC-Libya set out the test by which the Executive branch has sustained and upheld up until now.[94] It is unlikely that the Executive branch will soon (or ever) find cyberwarfare operations to fail the OLC-Libya test. Absent any contrary *legislation*, the OLC finds that Article II of the Constitution authorizes the President to use military force if they are serving an important U.S. interest, and that the operation be limited in nature, scope, and duration that fall below the threshold of an "act of war."[95]

The issue is that offensive cyberoperations make for a perfect presidential weapon. The first prong of the test is almost always met then, since the President can find any of myriad national interests given the long precedent of unchallenged military use. The second prong poses no challenge either,

92. *Id.*

93. *Id.*

94. Steven A. Engel, *April 2018 Airstrikes Against Syrian Chemical-Weapons Facilities*, 42 OP. OFF. LEGAL COUNSEL 10 (2018).

95. Scott R. Anderson, *Did the President Have the Domestic Legal Authority to Kill Qassem Soleimani?*, LAWFARE (Jan. 3, 2020, 4:49 PM), https://www.lawfareblog.com/did-president-have-domestic-legal-authority-kill-qassem-soleimani.

as by their very nature, cyberattacks are limited. Cyberweapons are specifically designed to accomplish only one task, for one system—no different than a programmed line of code. Cyberweapons are shallow in scope, they require neither troops on the ground nor cost very much in resources. Duration is no legal issue either, cyberattacks are as fast as the internet moves—a Cyber Command soldier's battle is fought and won in the time of a keystroke. Unlike a nuclear weapon or a drone strike there are no recorded cyberwarfare operations that have led to immediate mass casualty deaths. Cyberweapons are not conventional kinetic weapons.

However, Congress should not be content to sit back and allow the executive unfettered access to enjoy cyberweapons unregulated. In the past, Congress has failed to use the WPR to force presidential cooperation and consultation. It has lost control of entire *categories* of weapon systems to presidents. Congressional acquiescence has invited free use for presidents. By allowing lines to be drawn in the sand over whether boots are on the ground or not has allowed prior presidents to utilize bombers, fighter jets and armed drones (collectively henceforth known as "airpower") unchecked. Cyberweapons are the next evolution in a line of weapons that are also coincidentally conveniently designed to avoid the WPR, or Congressional cooperation generally. This Note does not seek to understate how important energetic and decisive control of the military under a single executive is. On the contrary, energetic, and decisive control of the military in a civilian Commander-in-Chief will afford great flexibility to respond quickly to threats against the United States. But this Note seeks to also stress the importance of an Executive who is not left unchecked.

When in 2020 then President Trump launched a drone strike that killed a senior Iranian military commander, he did not consult Congress.[96] The use of force was hard to defend, but was justified on the basis of OLC-precedent, and the fact that Congress has not ever challenged multiple similar situations in the past, such as in Syria and Kosovo.[97] While the Executive branch saw this as an act short of war, the United States Congress could have easily seen it as an act of war.[98] Yet, Congress' ability to reign in a president has been so long unexercised that it has essentially been abdicated.

The Constitution as it was written, and the War Powers Resolution as it is interpreted today, did not contemplate weapons that can be utilized as efficiently as cyberweapons. A looming constitutional crisis could be waiting

96. Christopher A. Preble, *Trump's Dangerous Escalation with Iran*, CATO INST. (Jan. 3, 2020, 9:40 AM), https://www.cato.org/blog/trumps-dangerous-escalation-iran.

97. Anderson, *supra*, note 95.

98. *Rep. Ro Khanna on Qassem Soleimani Assassination: Trump's Actions Are Unconstitutional*, DEMOCRACYNOW! (Jan. 3, 2020), https://www.democracynow.org/2020/1/3/rep_ro_khanna_on_qassem_soleimani.

for the Republic if (1) there remains no coordinated, informed cyber-defense that includes offensive cyberoperations that are legitimized by force of law and if (2) the separation of powers continues to erode as pertaining to novel weapons of war. If the trend continues, the separation of powers will only pertain to some branches of the military, or entire categories of weapons while ignoring others.

The President should be free to order the military to use offensive cyberoperations to decisively defeat adversaries in this wide domain that is actively being challenged. The President should be able to bear the force of a responsive, decisive military with clear guidelines on the use of this force. But this force is not theirs to regulate alone. Congress must play a more active role, even *if* their role is simply signing off on a flexible policy for use of cyberwarfare. The key difference is avoiding a perennial twilight in which the two separate political branches may one day end up in deep inter-branch conflict over crossing interpretations with deep repercussions, constituting a potential constitutional crisis. Congress and the Executive branch must be in lockstep, as constitutionally intended.

III. Recommendations For Creating A Constitutional Framework With Teeth That Effectively Responds To Foreign Cyberthreats

Cyberwarfare poses uniquely difficult issues. The best way to combat cyberwarfare is by countering adversarial foreign cyberoperations with offensive cyberwarfare operations.[99] Cyberwarfare inherently requires decisive, fast-acting responses superintended by a single hand, a role best fit for the President and their delegated subordinate commanders. However, there have been few guidelines laying out how to wield this unique power and none of our existing frameworks are compatible. Thus, Congress should seize this opportunity to strike while the iron is hot, create a new framework entirely, and reassert itself into the war powers debate before future incidents foreclose their participation, similar to how airpower assets came to be doctrinally separated after OLC-Libya.[100] Creating a statutory framework would not require reinventing the wheel—the subcomponent parts of an effective strategy are already well known and have been implemented throughout the government at various times.

99. *See* Joint Force Quarterly, *An Interview with Paul M. Nakasone*, Quarter 2019, at 4 (quoting General Nakasone: "[u]nlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it because that's what our adversaries are doing to us.").

100. Krass, *supra*, note 67, at 37.

A. Relying on the OLC Opinions: From Airpower to Cyberpower

OLC-Libya laid out a test that has been abused in the past but now may provide a strong structure for defending the offensive use of U.S. cyberoperations.[101] As noted above, U.S. presidents have been able to justify military action primarily due to the rationales that underpin the OLC-Libya opinion: absent legislation, the President may order military action prior to consulting Congress when serving an important national interest, if the operation will be limited in nature, scope, and duration that it falls below the threshold of an "act of war."[102]

Cyberoperations will not fall within the nature, scope, or duration of an act of war in the majority of circumstances. There are very few situations where one can imagine they would, especially considering precedential cases.[103] Arguably, the President should not be handcuffed from using cyberwarfare as part of their national defense or larger military strategy. Cyberwarfare is used by our adversaries, and the best way to defend against it is by investing in cyberwarfare capabilities of our own.

What evidence the military has accumulated demonstrates that the U.S. could use cyberwarfare to disable nuclear weapons, safeguard free elections, and discourage or punish invasions of allied nations.[104] In this way, cyberwarfare is no different than prior strategic uses of American military airpower. However, unlike airpower, cyberwarfare is not kinetic—meaning that its potential uses are far less lethal. This means that the U.S. could avoid larger collateral damages in accomplishing similar goals. Under the existing legal framework, the President will likely be able to continue to use cyberwarfare operations with great flexibility, in the interests of preserving American national power while promoting less bloodshed, and a more democratic world order. These are admirable, worthy goals.

However, this does *not* mean Congress should not participate in this process. Just because the majority of cyberoperations may not be construed as "acts of war" does not mean that it is not within the realm of possibility. Cyberwarfare is *not* entirely bloodless—*thus far* it has not been used in such a lethal fashion. The first airplanes were only used for mere scouting or

101. *Id.* at 27.

102. *Id.*

103. *Id.* at 32, 38 (describing U.S air operations over Bosnia to enforce a UNSC "no-fly zone" which led to flying over 2300 sorties, also referencing aerial bombing campaigns in Kosovo, both based on the President's constitutional authority nested in foreign relations and Commander-in-Chief powers, without specific prior approval from Congress).

104. THE PERFECT WEAPON (HBO Documentary Films 2020), at 66:16.

spying—today they easily level cities.[105] The possibility remains that like airpower assets, cyberwarfare may take on a more lethal tint in the future.[106]

Technologies advance and circumstances change. Congress should re-assert itself into the shared powers concerning the use of cyberwarfare before it gets away from Congress entirely, such as what has happened with air-power assets (i.e., drone strikes or no-fly zones). President Trump's strikes on Qassem Soleimani[107] and U.S. cyber-strikes on North Korean missiles off the East Sea[108] both demonstrate that the potential for a president to exercise an action that is, from their perspective, "short of war," but that could be seen as "acts of war" insofar as our adversaries, the international community or the United States Congress are concerned.

Put another way, the more tools and domains that Congress chooses to cede to the President as short of war-making (i.e., drone strikes, aerial bombing, DDoS attacks, malware attacks, etc.) the greater the probability that a president may eventually unilaterally use this power in an inappropriate way that undermines the position of the United States as whole. General Soleimani, while a hostile actor to the United States, was a member of Iran's uniformed military.[109] Insofar as executing a member of the military is concerned, it is entirely likely that the American people, and by extension, Congress *would* see this as an act of war. Because Congress has not challenged the President in the past and the courts have not enforced upon the President any such accountability, Congress would be forced to retroactively denounce one of its co-equal branches. This would be a Constitutional crisis. This potential for conflict makes a constitutional power struggle likely when paired with the unlimited potential of cyberweapons and cyberwarfare going forward.

The President requires flexibility, but Congress must reassert itself as a counterbalance. Congress may regret abdicating from the conversation yet again and should not do so.

---

105. The Editors of Encyclopaedia Britannica, *Military Aircraft*, BRITANNICA, https://www.britannica.com/technology/military-aircraft (last updated Oct. 31, 2018).

106. Melissa Eddy & Nicole Perlroth, *Cyber Attack Suspected in German Woman's Death*, N.Y. TIMES (Sept. 18, 2020), https:/www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.

107. Reuters-Dubai*, Iran vows revenge for Soleimani killing unless Trump put on trial*, REUTERS (Jan. 3, 2022) https://www.reuters.com/world/middle-east/iran-vows-revenge-soleimani-killing-if-trump-not-put-trial-2022-01-03/.

108. David E. Sanger & William J. Broad, *Trump Inherits a Secret Cyberwar Against North Korean Missiles*, N.Y TIMES (Mar. 4, 2017), https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html; Alex Lockie, *North Korea's embarrassing missile failure may have been due to US cyber sabotage*, INSIDER (Apr. 17, 2017), https://www.businessinsider.com/us-hack-north-korea-missile-system-2017-4.

109. The Editors of Encyclopedia Britannica, *Qassem Soleimani*, BRITANNICA, https://www.britannica.com/biography/Qassem-Soleimani (last updated Mar. 7, 2022).

B. Statutory Templates: National Defense Authorization Act for fiscal 2019, § 1642

In the summer of 2018, Congress passed the John McCain National Defense Authorization Act for Fiscal Year 2019, as Public Law 115-232.[110] The Act served as a fairly routine authorization of military appropriations under the Department of Defense.[111] Of note in NDAA 2019 was section 1642: "Active defense against the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, and Islamic Republic of Iran attacks in cyberspace" (hereinafter, the Active Defense Section, or ADS).[112]

The Active Defense Section validates the wisdom of a statutory authority to serve as an off-ramp to broadening presidential overreach with a legislative scheme as a path of least resistance and an exercise of "Jackson 1" unity. The ADS creates in section 1642(a) an authority to disrupt, defeat, and deter cyberattacks.[113] It created the National Command Authority (essentially the President and the Secretary of Defense) and used this entity to delegate Congressional authority to the executive branch. In this way, Congress essentially pre-authorizes "proportional" cyber operations in response to cyberattacks from adversaries.[114]

The Active Defense Section shows that Congress is increasingly aware of the murky waters 'short of warfare,' acknowledging the issue by creating a "mini-cyber AUMF" to address frustrations that the United States has not acted aggressively enough in response to foreign threats under both the Obama and Trump administrations.[115]

However, also reflecting Congress's traditional bullish caution, section 1642's Active Defense principle was *not* applied equally to all threat actors. Under the Active Defense Section, only four countries are outlined: Russia, China, Iran, and North Korea. Thus, the section only applies to these four nation-states. Given difficulties with attribution in cyber-space, this is a *striking* disadvantage. Cyberactors often go without recognition, and when they are recognized, their actions are often hidden through proxies. If a hypothetical cyber-attack originated from Pakistan, yet was sponsored, endorsed, or resourced by Iran, the Active Defense Section would prohibit the President from being able to execute a quick, responsive cyber-counter offensive. Certainly, if this is not the case, it is not made clear by the language

110. National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (2018).

111. *Id.*

112. *Id.* at 2132.

113. *Id.*

114. Robert Chesney, *The Law of Military Cyber Operations and the New NDAA*, LAWFARE BLOG (July 26, 2018, 2:07 PM), https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa.

115. *Id.*

of the statute. Regardless, the 2019-NDAA was an enormous step in the right direction, nonetheless.

The second issue with the 2019-NDAA had less to do with its substance and more to do with its medium. As an annual appropriations Act, the NDAA requires more active political participation from Congress. It further requires annual political consensus. In an era where Congressional politics are as divisive and polarized as ever, and where corrosive cyberwarfare focuses on democratic systems and degrading public trust, this may be a vulnerability. The latest edition of the NDAA, the National Defense Authorization Act for Fiscal Year 2022 became Public Law 117-81 in December of 2021 and is lacking the Active Defense section entirely, demonstrating the inconsistency of an annual application.[116]

Unfortunately, the 2019-NDAA ended up being a bit of a half-measure. However, like AUMF-Terror, it provides an interesting template for proposing a more permanent statutory fixture that addresses the same problem set.

C. Authorization for Military Force Cyber: How Congress Can Avoid Abdication

Instead of handcuffing the President by attempting to deny him the flexibility and diversity of options available under OLC-Libya and its underlying rationale, Congress can pass a legislative scheme that codifies the flexibility of OLC-Libya, tempered by additional restraints the same way the Active Defense section of 2019-NDAA was designed to do. If Congress authorizes a wide, flexible statute, future Presidents are more likely to use statutory authorizations instead of their inherent Article II powers. This creates a "path of least (political) resistance" for the Executive branch, by which they can achieve the vast majority of their goals with a Congressional stamp of preapproval. AUMF-Iraq and AUMF-Terror were used widely for over two decades to cover relevant military conflicts. A statutory authorization would look similar to AUMF-Terror, broad enough to cover multiple categories of offensive uses of cyberwarfare operations in the interest of the United States. Unlike AUMF-Terror, however, Congress should apply the lessons it learned in the past twenty years by designing more controls within a hypothetical AUMF-Cyber. AUMF-Cyber should be *deliberately* designed to last, unlike AUMF-Terror, which was *accidentally* designed to last.

AUMF-Cyber should incorporate a reasonable consultation requirement that echoes the same sort of engagement policy in the WPR and that was reflected in the Active Defense section of NDAA-2019. Unlike the WPR, an AUMF-Cyber consultation should be realistic: it should establish tiers of cyberoperations and should reserve Congressional consultation for

116. National Defense Authorization Act for Fiscal Year 2022, S.1605, 117th Cong. (2021).

only the *highest* tiers of cyberoperations. These highest tiers of operations should be those that mirror the effects of traditional kinetic strikes. This consultation requirement would preclude a sitting-president from using cyber-strikes in a way that mirrors the Soleimani strike, and protects Congress' Declare War powers, already interpreted into irrelevance in many other aspects of the national security domain.

Doctrinally, Congress does not only hang its hat on the Declare War clause, as mentioned above. Cyber-warfare is unique from airstrikes in that many of these foreign attacks uniquely target economic institutions and domestic infrastructure, including civilian businesses.[117] These are directly under Congress' ambit as well – and Congress has enumerated powers concerning the economy, including all channels of commerce.[118] Congress is also primarily responsible for propagating regulations for the Armed Forces.[119] Many claim this clause of the Constitution pertains only to administrative care over the military—though this is by no means the only valid viewpoint. Many legal scholars find that Constitutional text, structure, and history point to the contrary:

> Statutes regulating all of these matters depend on Congress's authority to structure the military, and at some times in the past Congress has exercised this power more aggressively than it has in current statutes. Congress should consider dusting off this item in its toolkit. In our brave new era of unstable politics and negative partisanship, amid potentially increasing pressures for short-sighted and politically motivated action, this congressional power may be one of the best means of encouraging caution and protecting good-government norms.[120]

Cyberoperations at the highest tiers are rare enough that it should not be seen as tactical micromanagement for Congress to set general guidelines in a prospective AUMF-Cyber, mirroring general rules of engagement. Congress is not telling individual soldiers to storm specific hills or destroy specific bunkers. It is declaring and setting broad policies regarding the use of a weapon that flits between warfare and espionage, a weapon that affects the

117. RA Atrews, *Cyberwarfare: Threats, Security, Attacks, and Impact,* 19:4, J. INFO. WARFARE 17, 24 (2020) (discussing that cyberwarfare has the potential to disrupt economies globally, costing the world economy $600 billion each year in losses, and the US economy up to $120 billion annually).

118. U.S. CONST. art. 1, § 8, cl. 3. (The Commerce Clause, which gives Congress the power "to regulate commerce with foreign nations, and among the several states, and with Indian tribes").

119. U.S. CONST. art. 1, § 8, cl. 14. (["The Congress shall have Powers…] To make Rules for the Government and Regulation of the land and naval Forces…").

120. Zachary Price*, Congress Has Broad Power to Structure the Military—and It Should Use It*, LAWFARE BLOG (Sept. 2, 2020, 10:31 AM), https://www.lawfareblog.com/congress-has-broad-power-structure-military-and-it-should-use-it.

global economy and interstate commerce as fluidly and quickly as it affects strategic military targets. There are many examples of Congress filling in significant decision making regarding military structure continuing into the 20th century.[121]

AUMF-Cyber would set the focus on offensive cyberoperations to a flexible standard, not dissimilar from the current test used by OLC-Libya. However, designing the test inside of a stand-alone statutory authority delegates Congressional authority regarding most routine cyberoperations. These are helpful because they avoid the Executive branch from padding itself thick with a widening body of unchallenged OLC interpretations affording the President more and more unilateral military power, anathema to a free Republic. By relying on statutory authority, this precedent regarding cyberwarfare is unlikely to grow. Meanwhile, the President remains free to delegate the authority to execute cyberoperations to lower combatant commands with a flexible berth, key to a unified national cyber-defense.

By creating an AUMF-Cyber that is separate from an annual defense authorization act (similar to section 1642's ADS of the 2019 NDAA), the statutory authority proposed here should be separate and unbound by an annual renewal requirement. It would not be affected by reactionary politics or fall hostage to partisan battles in Congress. Congressional cooperation would be important, but not perennially *crucial*, responding to the unfortunate political reality that Congress is often beset by inaction[122] Under a stand-alone statutory authority, that's fine.

Similarly, under this solution, judicial abstinence in refusing to take on highly political OLC opinions in Court would not be a deal breaker since the Executive branch is likely to take the path of least resistance that has been created for them, as evidenced by long-standing use of AUMF-Terror.

Establishing a clear policy and response rubric based in statutory authority signals to the world that the United States will respond to cyberattacks with offensive cyber-counteroperations, or equivalent necessary force. The 2011 International Cyberwarfare Strategy was the first breakthrough in setting such clear guidelines but did not hold the force of statutory law.[123] Congress cannot sit this out. By issuing its support to the President, Congress puts the President at Jackson 1: the very personification of sovereign power.[124] Ending this Constitutional "twilight" makes the American position

121. *Id.* (Discussing how Congress combined the Departments of the Navy and War into one Department of Defense and then authorized the President to establish "combatant commands" tied to particular missions.).

122. Greg Hadley, *2022 NDAA Hits More Hurdles in Senate as Continuing Resolution Deadline Looms*, AIR FORCE MAG. (Nov. 29, 2021), https://www.airforcemag.com/2022-ndaa-hits-hurdles-senate-cr-deadline-looms.

123. Theoharry, *supra*, note 11.

124. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

stronger overall, harder to divide politically, and reinforces a healthy separation of powers. Such a strong endorsement and promise of immediate retribution with similar offensive cyberoperations will deter many would-be attackers. This can replicate the success Cyber-Command enjoyed in 2018, while doing so in a way that maintains constitutional integrity.

Conclusion: Proactively Setting The Framework In A Time Of Calm Avoids A Constitutional Crisis In A Time Of Calamity

The OLC-Libya framework should be formally recognized as controlling for cyberwarfare operations and codified into a standing statutory scheme that keeps the spirit of section 1642 from the 2019-NDAA. This would afford the opportunity for the President to respond quickly. The latitude for this flexibility relies upon the long, rich precedent that finds deference in executive power, while acknowledging that prior understandings of what constitutes "warfare" may need to be updated. Cyberwarfare is an important toolkit as Presidents today leverage smart power strategies against geopolitical rivals.

This entire scheme and legal framework should be passed as legislation by Congress, and Congress should have an active hand in designing regulations on the use of offensive cyberwarfare as part of the national security strategy. Congress cannot abdicate its role and should begin a new precedent by taking a more assertive role in managing the use of military force. Setting limits now avoids future Presidents from abusing their powers later. It is vitally important that Congress reclaim their seat at the war powers table. This Note does not advocate for presidents to be stripped of their decision-making power. This Note also does not seek to idealize a world in which Congress can weigh in on every strategic military decision that weighs on the Commander-in-Chief. However, Congress can grant the President the latitude they request without abdicating from the conversation entirely. By creating a sturdy, thorough statutory authority such as an AUMF-Cyber, the President can feel comfortable knowing their superintendence of the military is still secure without feeling the need to push their inherent Article II powers further. They have already been pushed far enough in most other methods of war-making. Cyberwarfare should not be the next one—and it is unique and novel enough that Congress is not too late, if it acts now.

The United States faces threats today it has never faced before. The cyberwarfare threat is not to be underestimated. Cyberwarfare is no paper tiger, and the many unique ways it challenges the Republic are all potentially uniquely debilitating. It poses real threats to the economy, military, and democracy of the United States, ultimately posing a threat to a delicate balance with the Constitution of the United States itself. If the United States wants to defeat a threat unlike any it has ever seen before—it needs to boldly try

things it never has before. In the end, the constitutional integrity of the United States cannot afford to fold, and so it must adapt.

***