The Scholar: St. Mary's Law Review on Race and Social Justice

Volume 17 | Number 1 Article 33

1-1-2015

Mapping the Matrix: Defining the Balance between Executive Action and Legislative Regulation in the Battlefield of Cyberspace.

Tyler K. Lowe

MAPPING THE MATRIX: DEFINING THE BALANCE BETWEEN EXECUTIVE ACTION AND LEGISLATIVE REGULATION IN THE NEW BATTLEFIELD OF CYBERSPACE

TYLER K. LOWE*

* Tyler K. Lowe is a 2014 graduate of St. Mary's University School of Law, J.D., and a 2006 graduate of Texas A&M University, B.A. in American Studies. He currently serves as a Counsel in the United States Congress.

I. INTRODUCTION

On June 23, 2009, recently inaugurated President Barack Obama authorized the formation of The United States Cyber Command (USCYBERCOM) to protect the interests of the United States and conduct military operations in cyberspace.[1] USCYBERCOM was placed under the authority of The United States Strategic Command and tasked with centralizing the cyberspace operations of the Army, Air Force, Navy, and Marines.[2] Moreover, President Obama appointed the Director of the National Security Agency (NSA)—the lead federal agency for signal intelligence and information assurance[3]—to also serve as the Commander of USCYBERCOM.[4]

Almost four years later, at the end of President Obama's first term, then-Secretary of Defense Leon Panetta thrust USCYBERCOM, and the notion of cyber warfare, to the forefront of the American consciousness.[5] In a watershed speech before the Business Executives for National Security in New York City, Secretary Panetta branded cyberspace as the new frontier for the establishment of peace, security, and power in the twenty-first century.[6] Furthermore, the Secretary warned his audience, "cyber attacks are every bit as real as the more well-known threats like terror-

1. *See* President Barack Obama, Remarks by the President on Securing our Nation's Cyber Infrastructure (May 29, 2009) (transcript available at http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure) (announcing the creation of a new office at the White House to be led by the Cybersecurity Coordinator in a White House press release on May 29, 2009); *see also U.S. Cyber Command, Fact-sheets*, U.S. STRATEGIC COMMAND, http://www.stratcom.mil/factsheets/Cyber_Command (last updated Aug. 2013) (describing the creation and the mission of the United States Cyber Command).

2. *U.S. Cyber Command*, *supra* note 1.

3. *See About NSA: Mission*, NAT'L SEC. AGENCY, http://www.nsa.gov/about/mission/index.shtml (last updated Apr. 15, 2011) (describing the mission of the National Security Agency).

4. *See U.S. Cyber Command*, *supra* note 1 (listing National Security Agency Director, General Keith B. Alexander as the Commander of USCYBERCOM).

5. *See* Leon Panetta, U.S. Sec'y of Def., Remarks on the Global Threat of Cybersecurity to the Business Executives for National Security in New York City (Oct. 12, 2012) (transcript available at http://www.cfr.org/cybersecurity/secretary-leon-panettas-speech-cybersecurity/p29262) (stressing the importance and seriousness of the cyber warfare).

6. *See id.* ("Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and dangers.").

ism, nuclear weapons proliferation, and the turmoil that we see in the Middle East."[7]

During his speech, Secretary Panetta also laid the foundation of the Obama administration's approach to cyber warfare.[8] Without qualification, Secretary Panetta avowed the Department of Defense was prepared to respond to a "crippling cyber attack" and alternatively to pre-emptively strike if an imminent attack became apparent.[9] This signified a critical pivot in United States' cyber policy. For the first time in American history, the Executive Branch conceded that it was not merely limited to defensive operations in cyberspace.[10] Instead, Secretary Panetta acknowledged the ability of the United States military to wage an offensive cyber war.[11]

Around the same time as Secretary Panetta's speech, President Obama signed Presidential Policy Directive 20 (PPD-20).[12] This classified directive, which was later leaked by former NSA contractor Edward Snowden in June 2013,[13] establishes an Executive Branch framework for the approval of defensive and offensive cyber operations.[14] PPD-20 was authored in response to repeated failures by Congress to adopt legislation regulating cyber warfare.[15]

Before the disclosure of PPD-20, an undisclosed legal review of the United States' approach to cyber warfare affirmed the widely accepted power of the President to order a pre-emptive strike to quell an imminent cyber attack.[16] However, the release of PPD-20 unveiled the true extent

---

7. *Id.*

8. *See generally id.* (discussing the dynamics of the broad approach taken by the Executive Branch to combat cyberwarfare).

9. *Id.*

10. Carlo Munoz, *Panetta Acknowledges US has the Capacity to Wage Cyber Warfare*, THE HILL (Oct. 12, 2012), http://thehill.com/blogs/hillicon-valley/technology/261705-panetta-unveils-aggressive-new-cyberwarsafre-strategy.

11. *Id.*

12. Carlo Munoz, *Obama Authorizes New Cyber Warfare Directive*, THE HILL (Nov. 14, 2012), http://thehill.com/blogs/defcon-hill/policy-and-strategy/267879-report-obama-authorizes-new-cyber-warfare-directive.

13. Glenn Greenwald et. al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

14. *See generally* Glenn Greenwald & Ewan MacAskill, *Obama Orders US to Draw up Overseas Target List for Cyber-Attacks*, THE GUARDIAN (Jun. 7, 2013), http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas (highlighting the top-secret operational standards for cyber warfare in PPD–20).

15. *See* Munoz, *supra* note 12 (mentioning that the PPD-20 compensates for the failure of Congress to pass legislation to close gaps in the nation's cyber warfare policy).

16. *See* David E. Sanger & Thom Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, N.Y. TIMES (Feb. 3, 2013), http://www.nytimes.com/2013/02/04/us/broad-powers-

of the President's self-granted authority to conduct cyber warfare: the President reserves the right to utilize the cyber arsenal for defensive and offensive operations without delineating bright line thresholds for either type of attack.[17] The Executive Branch failed to define when a threat becomes so imminent as to allow for defensive attacks and provided only an amorphous "[United States] national objectives around the world" standard for when offensive attacks could be undertaken by U.S. personnel.[18]

As recently as February 2013, it was believed that President Obama had only employed the cyber arsenal once during his presidency, to attack the Iranian nuclear facility at Natanz.[19] However, budget documents leaked by Edward Snowden in August 2013[20] indicate the United States conducted 231 cyber operations in 2011 alone.[21] While information is not currently available to determine what percentage of the 231 cyber operations were used for intelligence gathering versus infrastructure destruction, it is apparent the Obama Administration has wholeheartedly embraced defensive and offensive cyber tactics as a part of the national security apparatus.[22]

The language of PPD-20 pays lip service to compliance with domestic law, but it does not include any provisions for congressional approval of cyber war.[23] Instead, presidential support is the highest level of approval expressly required.[24] Therefore, an attack, possibly tantamount to an act of war, could be perpetrated by the United States without the approval of the Legislative Branch. This unchecked authorization process, specifically applying to cyber attacks, could produce "significant consequences," such as "loss of life, significant responsive actions against the United

---

seen-for-obama-in-cyberstrikes.html?pagewanted=all&_r=0 (recognizing the authority of the President to respond to an imminent cyber attack on the United States).

17. *See generally* PRESIDENTIAL POLICY DIRECTIVE/PPD–20 ON U.S. CYBER OPERATIONS POLICY FOR THE VICE PRESIDENT ET AL. (Oct. 2012), *available at* http://www.fas.org/irp/offdocs/ppd/ppd-20.pdf (omitting any discernable standard for imminent threat or the definition of an action in furtherance of national interests).

18. Greenwald & MacAskill, *supra* note 14; *see also* PRESIDENTIAL POLICY DIRECTIVE/PPD–20, *supra* note 17 (detailing the thresholds, or lack thereof, for defensive and offensive cyber operations).

19. Sanger & Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, *supra* note 16.

20. Greenwald et. al., *supra* note 13.

21. David E. Sanger, *Budget Documents Detail the Extent of U.S. Cyberoperations*, N.Y. TIMES (Aug. 31, 2013), http://www.nytimes.com/2013/09/01/world/americas/documents-detail-cyberoperations-by-us.html.

22. *See id.* (deriving the Obama administration's reliance upon cyber operations from the numerous attacks launched in 2011).

23. *See* Greenwald & MacAskill, *supra* note 14 (mentioning only that presidential approval, and not congressional, is needed for the most intrusive cyber attacks).

24. *Id.*

States, significant damage to property, serious adverse U.S. foreign policy consequences, or serious economic impact on the United States."[25]

Through both the Bush and Obama administrations, Congress has been unable to pass comprehensive legislation regulating cyber war.[26] As a result of congressional silence, the Obama administration has been forced to articulate the current cyber warfare structure and polices of the United States, as seen in PPD-20. As one senior administration official recently said, "Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces."[27] And, as this article will argue, once a navy, air force, or cyber military is built, accompanying regulations are also needed.

The current, virtually unchecked authority of the President to conduct defensive and offensive cyber attacks is a natural byproduct of the Executive Branch drafting the domestic rules for cyber warfare. Thus, the Legislative Branch must act to impose original or existing regulations to rein in this novel and developing authority of the President.

II. WHAT IS CYBER WAR?

National security expert Richard A. Clarke defines cyber war as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[28] Alternatively, the Joint Chiefs of Staff define "Cyber Warfare" as "[a]n armed conflict conducted in whole or part by cyber means" and "[m]ilitary operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict."[29] When compared, these definitions present three prerequisites for cyber war.[30] Such prerequisites help to differentiate cyber war from lesser cyber attacks, cyber-

25. Presidential Policy Directive 20, U.S. CYBER OPERATIONS POLICY, 9 (Oct. 16, 2012), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

26. *See generally* JOHN ROLLINS & ANNA C. HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS (2009) (discussing the abundance of Executive Branch action and lack of legislative input in the developing field of cyber warfare).

27. Greenwald & MacAskill, *supra* note 14.

28. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 6 (First Ecco Paperback ed. 2012).

29. Memorandum from James E. Cartwright, Gen., U.S. Marine Corps, on Joint Terminology for Cyberspace Operations to the Chiefs of the Military Services, Commanders of the Combatant Commands, & Directors of the Joint Staff Directorates 8 (2011), *available at* http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

30. *See* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 82236–37 (2012) (classifying cyber operations to determine which actions rise to the level of a cyber attack, in the context of cyber warfare).

espionage, and cybercrime—an important distinction because these latter subsets of cybersecurity are subjected to different domestic and international legal strictures.[31]

The first prerequisite for cyber war is that there must be a cyber attack by or upon a nation.[32] A cyber attack is defined as "any action taken to undermine the functions of a computer network for a political or national security purpose."[33] The second prerequisite is the cyber attack must be tantamount to an "armed attack" in traditional-kinetic warfare.[34] A cyber attack is equivalent to an armed attack when physical injury, death, or significant destruction is the proximate result of a cyber assault.[35] The final prerequisite is that if a cyber attack does not rise to the level of an armed attack, it may still fall beneath the umbrella of cyber war if it occurs within the framework of a conventional armed conflict.[36]

PPD-20 further defines cyber attacks by classifying them into two categories: defensive and offensive operations.[37] Defensive cyber attacks are used to safeguard against imminent cyber or kinetic "threats or ongoing attacks" counter to the interests of the United States.[38] Conversely, offensive cyber operations are loosely defined as actions "that are intended to enable or produce cyber effects outside United States Government networks" and do not include defensive measure or intelligence collection.[39] Cyber effects include "[t]he manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[40]

---

31. *See generally id.* (analyzing different actions in cyberspace in an effort to define cyber attack and lesser cyber incidents).

32. *See id.* at 836–37 (classifying cyber operations to determine which actions rise to the level of a cyber attack, in the context of cyber warfare).

33. *Id.* at 826.

34. *Id.* at 836–37.

35. *See* Aram Roston, *U.S.: Laws of War Apply to Cyber Attacks*, ARMY TIMES (Sept. 18, 2012), http://www.armytimes.com/article/20120918/NEWS/209180311/U-S-Laws-of-war-apply-to-cyber-attacks (reporting on the comments of United States Department of State legal advisor Harold Koh regarding the domestic and international legal strictures applicable to cyber warfare).

36. *See* Hathaway et al., *supra* note 30, at 836–37 (classifying cyber operations to determine which actions rise to the level of a cyber attack, in the context of cyber warfare).

37. PRESIDENTIAL POLICY DIRECTIVE/PPD–20, *supra* note 17.

38. *Id.*

39. *Id.*

40. *Id.*

III. The Scope of Legislative Authority to Authorize Cyber War

A. *Textual and Judicial Support for Congressional Power to Authorize War*

i. The Constitution and Related Texts

Article I, Section Eight of the Constitution of the United States vests in Congress the power "[t]o declare War."[41] Alternatively, the President is empowered to conduct, or "make," war.[42] This dichotomy was installed to prevent the President from attaining the unilateral war powers of the British monarchy.[43] Congressional authorization was intended to slow the march to war and prevent any one individual from possessing the sole power to commit the nation to armed conflict.[44]

George Washington and his contemporaries believed congressional authorization was a prerequisite for the use of force that was not conducted in self-defense.[45] In response to Native American attacks on the western frontier, President Washington stated: "The Constitution vests the power of declaring war with Congress; therefore no offensive expedition of importance can be undertaken until after they shall have deliberated on the subject, and authorized such a measure."[46]

Congress has only declared war five times in the history of the United States.[47] Obviously, these conflicts do not encompass the entirety of U.S.

---

41. U.S. Const. art. I, § 8.

42. *See* U.S. Const. art. 2, § 2 (expressly stating "[t]he President shall be Commander-in-Chief of the Army and Navy of the United States, and of the Militia of the several States").

43. *See* The Federalist, No. 69, 418 (Alexander Hamilton) (Bantam Classic ed., 1982) (discussing the resemblance of the power granted to the President and the power of Great Britain's monarch while also highlighting the purposeful differences).

44. *See* 2 The Documentary History of the Ratification of the Constitution by the States—Pennsylvania 583 (Merrill Jensen ed., 1976) (examining the importance and necessity of the division of war powers between the president and Congress).

45. *See* 33 George Washington, The Writings of George Washington from the Original Manuscript Sources 73 *available at* http://web.archive.org/web/20110220233049/http://etext.lib.virginia.edu/etcbin/toccer-new2?id=WasFi33.xml&vimages=images/modeng&data=/texts/english/modeng/parsed&tag=public&part=59&division=div1 (John C. Fitzpatrick ed., 1997) (including President George Washington's thoughts on offensive measures against the Creek Nation necessitating an evaluation and authorization by Congress).

46. *Id.*

47. *See* Curtis A. Bradley & Jack L. Goldsmith, Foreign Relations Law 221 (4th ed. 2011) ("[T]he War of 1812; the Mexican–American War of 1846–48; the Spanish–American War of 1898; World War I; and World War II.").

military action over the preceding two centuries.[48] Instead, Congress either approved a lesser "use of force," rather than a full declaration of war, or remained silent.[49]

The classic view of the early presidents, requiring congressional approval, must be juxtaposed with the modern view of unilateral executive action.[50] This assessment, most famously forwarded by Professor John Yoo, claims the Declaration of War Clause was merely intended as a trigger for rights and procedures under international law, and not a limit on executive power.[51] Rather, the true authority of Congress to restrain presidential war-making power lay in its ability to manage the budget of the armed forces.[52] This can be seen in Article I, Section Eight of the U.S. Constitution, which empowers Congress to "raise and support Armies."[53] Moreover, *The Federalist Papers*, specifically numbers 24 and 25, clearly charge Congress with this vital national security task.[54] *Federalist 24* reserves the autonomous authority to create and fund military forces for Congress,[55] while *Federalist 25* articulates the importance of standing armies in times of peace and war.[56] The author, Alexander Hamilton, urged his readers not to be "dupes" in their reliance on militias to provide the requisite protection for the nation.[57] Mr. Hamilton further declared the nation must be prepared to counter the might of a "regular

48. *See id.* ("[T]he United States has utilized military force in hundreds of situations not involving declarations of war.").

49. *See id.* (enumerating the instances of United States military engagement, both declared and undeclared, on the international stage).

50. *See id.* at 223–24 (analyzing the different views of the power the Declare War Clause of the Constitution grants the Legislative Branch to sanction war).

51. *See* John Yoo & James C. Ho, *Essays on Article I: Declare War*, *The Heritage Guide to the Constitution*, THE HERITAGE FOUND., http://www.heritage.org/constitution#!/articles/1/essays/49/declare-war (last visited June 12, 2014) (asserting an Executive Branch-centric viewpoint on the constitutional authority of Congress to declare war).

52. *See* BRADLEY & GOLDSMITH, *supra* note 47, at 224 (quoting Yoo, in regards to Constitutional power to wage war, "that Congress retains an ultimate check on presidential power through its appropriations power").

53. U.S. CONST. art I, § 8, cl. 12.

54. *See* BRADLEY & GOLDSMITH, *supra* note 47, at 209–10 (showing the constitutional assignment of congressional war powers as discussed in *The Federalist Papers*).

55. *See* THE FEDERALIST, No. 24, 138 (Alexander Hamilton) (Bantam Classic ed., 1982) (analyzing the division of authority regarding the United States military and specifically highlighting the exclusive power of the legislature to raise and support an army and navy).

56. *See* THE FEDERALIST, No. 25, 143 (Alexander Hamilton) (Bantam Classic ed., 1982) (forwarding the argument a perpetually standing military, even in times of peace, gains more experience and therefore can better protect and serve the national security interests of the United States).

57. *Id.*

and disciplined army" with a potent force of the same ilk.[58] In a harbinger of future defense philosophies Mr. Hamilton said: "War, like most other things, is a science to be acquired and perfected by diligence, by perseverance, by time, and by practice."[59]

ii. Judicial Development of Congressional Authority

Three important cases, *Bas v. Tingy*,[60] *Little v. Barreme*,[61] and *Orland v. Laird*,[62] which spanned from the undeclared war with France to the Vietnam War, further developed the constitutional power conferred upon Congress to authorize war.[63]

In *Bas v. Tingy*,[64] the Supreme Court addressed the status of an "enemy" nation in the absence of an official declaration of war.[65] The Court divided public war, which it defined as any government-approved use of force between two nations, into two categories: public general war and public qualified war.[66] In a general war, a formal declaration has occurred and both nations are authorized "to commit hostilities against all the members of the other, in every place, and under every circumstance[;] . . . and all the rights and consequences of war" are attached to their actions.[67] But, in a qualified war, no official declaration has occurred and the militaries and persons of both nations are restrained in their actions.[68] This limitation does not, however, preclude the existence of an actual war.[69]

In essence, Congress may thus authorize a restricted war against a foreign nation by a decree of less substantiality than a formal declaration of war, while the Executive is restricted within the bounds established by

58. *Id.*

59. *Id.*

60. Bas v. Tingy, 4 U.S. 37 (1800).

61. Little v. Barreme, 6 U.S. (2 Cranch) 170 (1804).

62. Orlando v. Laird, 443 F.2d 1039 (2d Cir. 1971).

63. *See generally* BRADLEY & GOLDSMITH, *supra* note 47, at 211–21 (depicting the judicial evolution of the constitutional clause that grants Congress the authority to Declare War).

64. *Bas*, 4 U.S. 37.

65. *See generally* BRADLEY & GOLDSMITH, *supra* note 47 (discussing congressional and Executive Branch action regarding the military during the undeclared war with France).

66. *See Bas*, 4 U.S. at 40, 44 (differentiating between the status and rights of enemy nations during times of war that have been formally authorized and hostilities that have not received full a declaration of approval).

67. *Id.* at 40.

68. *See id.* at 40–41.

69. *See id.* (noting that although hostilities are limited between two powers, the conflict remains a "public war" in which there is "an external contention by force, between some of the members of two nations, authorized [sic] by the legitimate powers").

the Legislative Branch.[70] This restraint on presidential authority was reaffirmed four years later in the second important case, *Little v. Barreme*,[71] and still stands as good law.[72]

The third important case, *Orland v. Laird,* is a Second Circuit Vietnam-era case that expressed three significant judicial interpretations of the legislative power to authorize war.[73] First, the court of appeals held congressional authorizations of war do not have to be expressly stated.[74] Instead, legislative permission may be inferred from collaboration between the President and Congress, and congressional participation in the preparation and execution of war.[75] Second, the court acknowledged that an express declaration of war, when both branches are in agreement about the necessity of action, would be burdensome, unnecessarily constrain the President, and be contrary to the interests of the nation.[76] Finally, the court expressed its discomfort with forcing Congress and the President to adopt a clear mechanism for declarations of war, for fear it would impinge upon the flexibility and independence of the two political branches.[77]

Therefore, after *Orlando v. Laird*, congressional authority to declare war no longer requires a formal declaration of war.[78] Instead, an authorization of force is adequate to permit action by the President.[79] This authorization may be inferred from legislation, appropriations, and congressional consent to executive operations.[80] Thus, the independent legislative duty to raise and support armies now serves as evidence of congressional authorization for the use of force in a qualified war.

---

70. *See* Bas *id.* at 40 (affirming that "those who are authorized to commit hostilities, act under special authority, and can go no farther than to the extent of their commission").

71. Little v. Barreme, 6 U.S. (2 Cranch) 170 (1804); *see* Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 157 (2010) (exploring the role of Congress in determining when the United States should enter into a military conflict).

72. Dycus, *supra* note 71, at 157 (stating that since Little v. Barreme no court has ruled otherwise).

73. Orlando v. Laird, 443 F.2d 1039 (2d Cir. 1971).

74. *Id.* at 1043.

75. *See id.* at 1042–43 (finding an express declaration of war from the Legislative Branch no longer necessary to formally authorize war; a declaration may be inferred from congressional action such as the appropriation of $700 million for use "upon determination by the President that such action is necessary in connection with military activities in Southeast Asia").

76. *Id.* at 1043.

77. *Id.*

78. *Id.* at 1042–43.

79. *Id.*

80. *Id.*

B. *Congressional Initiatives to Authorize Cyber War*

To date, Congress has not issued a formal declaration of cyber war against a foreign nation, nor has it authorized a lesser use of cyber force against an enemy state.[81] However, the 2001 Authorization for the Use of Military Force[82] could provide congressional approval for cyber warfare aimed at al-Qa'eda, the Taliban, or associated forces.[83]

Traditionally, legislation on cyber issues has been limited to the cybercrime offenses and penalties, and the establishment of administrative procedures to prevent cyber attacks on executive agencies.[84] But, in the National Defense Authorization Act for Fiscal Year 2012 (NDAA-FY12), Congress officially recognized the ability of the Executive Branch to conduct offensive cyber warfare:

Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution.[85]

While not a formal declaration of war or specific authorization of force, this language could be construed as an example of inferred approval for the use of cyber force.[86] Congress reiterated its support for presidential authority to initiate cyber war in the National Defense Authorization Act for Fiscal Year 2013 (NDAA-FY13).[87]

These authorizations resolved two issues regarding cyber warfare. First, they laid the foundation for executive authority to conduct offensive cyber operations.[88] Second, the acts were a precondition for the ap-

---

81. Dycus, *supra* note 71, at 157.

82. Authorization for Use of Military Force, Pub. L. No. 107–40, 115 Stat. 224 (2001).

83. *See* ROLLINS & HENNING, *supra* note 26, at 9, 12 (listing presidential authorities that could be used to justify unilateral Executive Branch implementation of cyber warfare operations).

84. *See id. at* 3–5 (cataloging previous attempts by Congress to legislate protections from cyber attacks).

85. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

86. *See* Orlando v. Laird, 443 F.2d 1039, 1042–43 (2nd Cir. 1971) (explaining that congressional action can be interpreted as authorization from Congress the making of war).

87. *See* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112–239, § 940, 126 Stat. 1632, 1888–89 (2013) (reaffirming the congressional recognition of presidential power to conduct offensive cyberwarfare).

88. *See* National Defense Authorization Act for Fiscal Year 2012 § 954, 125 Stat. at 1551 ("Congress affirms that the Department of Defense has the capability, and *upon direction by the President may conduct offensive operations* in cyberspace to defend our Nation, Allies and interests") (emphasis added).

propriation of funds to support the designated activity.[89] Accordingly, after the passage of NDAA-FY12 the Executive Branch officially possessed the authority to conduct offensive cyber operations, so long as they conformed to the traditional rules of armed conflict and the War Powers Resolution.[90]

Congress provides defense appropriations legislation to fund the activities and programs enumerated in the NDAA.[91] In fiscal year 2013, the Department of Defense utilized $3.9 billion of its appropriated funds for cyber operations.[92] In 2014, the Department requested a twenty percent increase to $4.7 billion. .[93] Additionally, defense officials plan to increase the number of USCYBERCOM employees from 900 to 4,900[94] and have made it abundantly clear that cyber warfare funding will not be affected by forced-sequestration cuts.[95]

Essentially, Congress has raised and supported a standing cyber army, and its authorizations for the use of offensive force infer a grant of authority upon the Executive Branch. Therefore, continued appropriations for cyber warfare operations, coupled with the power conveyed in NDAA-FY12 and NDAA-FY13, provide the Executive Branch with the authority to employ offensive cyber force.

---

89. *See Budget Process: Authorization vs Appropriation*, U.S. SENATE COMMITTEE ON APPROPRIATIONS, http://www.appropriations.senate.gov/content/budget-process (last visited August 13, 2014) (defining the purpose of congressional authorizations).

90. *See* National Defense Authorization Act for Fiscal Year 2012 § 954, 125 Stat. at 1551 ("[U]pon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, *subject to*—(1) *the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and* (2) *the War Powers Resolution.*") (emphasis added).

91. *See Budget Process*, U.S. SENATE COMMITTEE ON APPROPRIATIONS ("For discretionary spending, the role of the authorizing committees is to enact legislation that serves as the basis for operating a program and that provides guidance to the Appropriations Committees as to an appropriate level of funding for the program.").

92. *See* Jim Michaels, *Pentagon Expands Cyber-Attack Capabilities*, USA TODAY (Apr. 21, 2013), http://www.usatoday.com/story/news/nation/2013/04/21/pentagon-expanding-offensive-cyber-capabilities/2085135/ (detailing the funds used and requested by the Department of Defense for cyber warfare operations).

93. *See id.* (detailing the funds used and requested by the Department of Defense for cyberwarfare operations).

94. Tom Gjelten & Audie Cornish, *All Things Considered: Pentagon to Dramatically Expand 'Cyber Warrior' Force*, NATIONAL PUBLIC RADIO (Jan. 28, 2013), http://www.npr.org/2013/01/28/170494486/pentagon-to-dramatically-expand-cyber-warrior-force.

95. *See* Elisabeth Bumiller & Thom Shanker, *Defense Budget Cuts Would Limit Raises and Close Bases*, N. Y. TIMES (Jan. 26, 2012), http://www.nytimes.com/2012/01/27/us/pentagon-proposes-limiting-raises-and-closing-bases-to-cut-budget.html?pagewanted=1&_r=0 (reporting the Obama Administration's steadfast support of cyber warfare operations, despite across-the-board budget cuts).

IV. The Scope of Executive Authority to Make Cyberwar

A. *Textual and Judicial Support for Presidential Power to Make War*

i. Constitutional Origins of Executive Power

The entirety of "[t]he executive Power" of the United States is vested solely in the President.[96] This grant of authority is broader than that of Congress, which is limited to a list of enumerated powers.[97] Consequently, constitutional scholars generally agree the President possesses expansive power to conduct international affairs, including war, except where constitutional authority is reserved to Congress.[98]

The war power of the Executive is buttressed by Article II, Section Two, Clause One, which appoints the President as "Commander in Chief" of the armed forces.[99] Consequently, the President is charged with "the supreme command and direction of the military and naval forces, as first General and admiral" of the United States.[100] The Executive was vested with this unilateral power to provide for efficient and responsive decision-making by a single individual rather than a committee.[101] As the Supreme Court stated in *United States v. Curtiss-Wright Corp.*, the President, as leader of the military, diplomatic, and intelligence corps, is uniquely positioned with the knowledge and ability to act as the "sole organ of the nation" for external affairs.[102]

ii. Defensive Versus Offensive War Capabilities

There is a dearth of law defining when the President may instigate military action without congressional approval.[103] This is largely the result of judicial reluctance to interfere with the political decisions of the Execu-

---

96. U.S. Const. art II, § 1, cl. 1.

97. *See* Yoo & Ho, *supra* note 51 (claiming the constitutional grant of war making authority to the president is more expansive than that afforded to Congress).

98. *Id.*

99. U.S. Const. art II, § 2, cl. 1.

100. The Federalist, No. 69, 418 (Alexander Hamilton) (Bantam Classic ed., 1982).

101. *See* Yoo & Ho, *supra* note 51 (alleging history supports the proposition of an individual, rather than a committee of leaders, making military decisions in a time of war).

102. *See* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 319 (1936) (quoting John Marshall in an argument he made to the House of Representatives on March 7, 1800).

103. *See* Erwin Chemerinsky, Constitutional Law: Principles and Policies 381 (4th ed. 2011) (acknowledging the absence of judicial decisions concerning either the use of unilateral Executive Branch action to initiate military operations or the power of Congress to halt preexisting military engagement).

tive and Legislative Branches.[104] The federal courts have continuously categorized judicial challenges to foreign policy and the use of war powers as nonjusticiable political questions.[105]

Nonetheless, as Commander-in-Chief, the President is constitutionally vested with the authority to lead U.S. military operations.[106] This includes the right to lead in both defensive and offensive actions.[107] It is generally accepted that to initiate or conduct defensive operations no authorization from Congress is required, so long as they are conducted in response to an actual harm or imminent threat.[108] On the other hand, to initiate or conduct offensive measures he may be required to get congressional approval.[109]

James Madison first championed the defensive capabilities of the Executive Branch during the drafting of the Constitution.[110] Mr. Madison moved to replace the phrase "make war" with "declare war," in the enumeration of Legislative powers, to preserve the authority of the President to "repel sudden attacks."[111] The Supreme Court later recognized this power in *The Prize Cases*.[112]

The Prize Cases decision denied the President the "power to initiate or declare a war," but it did allow for unilateral executive action in the event of "invasion by foreign nations."[113] In fact, the Court found that the President is bound by the Constitution to repel a use of force with force.[114] In furtherance of this duty, the Executive Branch alone is to

---

104. *See id.* (attributing judicial reluctance to weigh in on war powers to the doctrine of political question, which deems these issues are best left to the Executive and Legislative Branches of the government to decide).

105. *See id.* (attributing judicial reluctance to weigh in on war powers to the doctrine of political question, which deems these issues are best left to the Executive and Legislative Branches of the government to decide).

106. U.S. CONST. art II, § 2, cl. 1.

107. *See* The Prize Cases, 67 U.S. 635, 668 (1863) (stating the President "is the Commander in chief of the Army and Navy of the United States, and of the militia of the several States when called into the *actual service* of the United States").

108. *Id.*

109. *See id.* (defining situations where the Constitution either limits Executive Branch power to initiate war or affords the president authority to conduct military operations without prior approval from Congress).

110. *See* 2 THE RECORDS OF THE FEDERAL CONVENTION OF 1787 318–319 (Max Farrand ed., 1911) (documenting Mr. Madison's participation in the debate on the power of government to "make" or "declare" war).

111. *Id.* at 318.

112. *See generally* The Prize Cases, 67 U.S. 635 (asserting the President's authority to act without congressional approval in the case of the militant attack on the United States).

113. *Id.* at 668.

114. *See id.* (defining situations where the Constitution either limits Executive Branch power to initiate war or affords the president authority to conduct military operations without prior approval from Congress).

decide the details of a proportional retaliation.[115] Thus, when the United States is attacked, the President is obligated to formulate a response, and there is no requirement he wait for Congress to "baptize" the conflict with a formal authorization.[116]

Presidential authority to repel sudden attacks has traditionally been limited to acts of "anticipatory self-defense."[117] Former Secretary of State Daniel Webster established U.S. guidelines for anticipatory self-defense in an 1842 diplomatic note regarding the sinking of an American ship by British forces.[118] Secretary Webster proclaimed "anticipatory action" is allowable only when "the necessity of that self-defense is instant, overwhelming, and leaving no choice of means and no moment for deliberation."[119] Therefore, within these parameters, the President is permitted to initiate defensive military action when an attack from a foreign nation is imminent and there is no time to pursue non-military options.[120] Fast approaching warplanes and armed forces marching toward a border are both examples of imminent attacks.[121]

However, in the wake of the terrorist attacks of September 11, 2001, the United States announced a new strategy of pre-emptive self-defense.[122] The United States National Security Strategy of September 2002 stated, "To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary act pre-emptively" and "as a matter of common sense and self-defense, America will act against such emerging threats before they are fully formed."[123] Consequently, the authority of the President to conduct defensive military operations has been extended, because the imminence prerequisite is either significantly diminished or entirely discarded.[124]

---

115. *Id.* at 670.

116. *Id.* at 669.

117. *See* STEPHEN C. MCCAFFREY, UNDERSTANDING INTERNATIONAL LAW 242–43 (2006) (discussing actions which gives rise to self-defense, specifically triggers for anticipatory and pre-emptive self-defense, and the recent policy transition of the United States from the former to the latter).

118. *Id.* at 243.

119. A DIGEST OF INTERNATIONAL LAW 412 (John Basset Moore ed., 1906).

120. *See* MCCAFFREY, *supra* note 117, at 243 (remarking that Mr. Webster's statement "has been widely accepted as an authoritative statement relative to the customary law of self-defense and was referred to approvingly by the Nuremburg Tribunal").

121. *Id.* at 242.

122. *Id.*

123. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (Sept. 2002), *available at* http://www.state.gov/documents/organization/63562.pdf.

124. *See* MCCAFFREY, *supra* note 117, at 242–45 (discussing the adoption of the policy of pre-emptive self-defense articulated by the U.S. National Security Strategy issued in

Alternatively, the President may conduct offensive military operations supported by a congressional declaration of war or authorization for the use of force.[125] Therefore, the Executive may utilize armed force, without any basis in self-defense, to the extent authorized by the Legislative Branch.[126] Nevertheless, modern presidents have continually claimed the ability to "commit US troops abroad" and "take military action" for the protection of "important national interests," without prior congressional authorization.[127] The foundation for this assertion of authority is said to arise from the Chief Executive and Commander-in-Chief clauses of Article II, coupled with more than two centuries of practice.[128] Accordingly, executive officials have argued the "historical gloss" on the Constitution is rife with presidential uses of force sans approval from Congress.[129] And, presidential attorneys argue, this practical application informs constitutional interpretation.[130] However, executive representatives acknowledge that the President is constitutionally precluded from initiating military action, even for the protection of national interests, when it would be equivalent to war, as described in the Article I Declaration of War Clause.[131] Hence, the President must conduct a fact-specific analysis of the "anticipated nature, scope, and duration" of a potential military action to determine whether it is tantamount to war.[132] If it would be tantamount to war, a declaration from Congress is required.[133]

If the President wishes to initiate military operations without congressional authorization, the administration must conduct a two-pronged

---

September, 2002, and suggesting that "the use of force in pre-emptive self-defense does not appear to be permissible either under Article 51 or under customary international law").

125. *See* The Prize Cases, 67 U.S. 635, 668 (1863) (stating "Congress alone has the power to declare a national or foreign war" but the President "is the Commander in chief of the Army and Navy of the United States, and of the militia of the several States when called into the *actual service* of the United States").

126. *See generally* Bas v. Tingy, 4 U.S. 37 (1800) (differentiating in the status and rights of enemy nations during times of war that have been formally authorized as opposed to hostilities that have not received full a declaration of approval).

127. Memorandum Opinion from Caroline D. Krass, Principal Deputy Assistant Attorney Gen., on Authority to Use Military Force in Libya to the Attorney Gen. 6 (Apr. 1, 2011), *available at* http://graphics8.nytimes.com/packages/pdf/world/20110401-authority-military-use-in-libya.pdf.

128. *Id.*

129. *See id.* (discussing the "historical glass" on the power of the Executive Branch specifically).

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.* at 9.

analysis.[134] First, the Executive must determine whether a significant national interest is served to allow the President to utilize Chief Executive and Commander-in-Chief authority.[135] The protection of American citizens and property,[136] regional stability, and the credibility of international organization and treaties are historical examples of sufficient national interests.[137]

Second, the President must determine whether the nature, scope, and duration of the desired operation are extensive enough to require a congressional authorization of war.[138] This multi-faceted analysis is unique for each situation, but will usually include such queries as: how many ground troops are required; what is the end goal of the mission; what is the risk of escalation; is sustained conflict foreseeable; and, whether there is a plan for withdrawal.[139]

---

134. *See id.* at 10 (relying on the framework established by Supreme Court precedent, "the President's legal authority to direct military force . . . turns on two questions: first, whether United States operations . . . would serve sufficiently important national interest to permit the President's action as Commander in Chief and Chief Executive and pursuant to his authority to conduct U.S. foreign relations; and second, whether the military operations that the President anticipated ordering would be sufficiently extensive in 'nature, scope, and duration' to constitute a 'war' requiring prior specific congressional approval under the Declaration of War Clause").

135. *See id.* (following Supreme Court precedent, the President's legal authority to use military force in Libya turned first on "whether United States operation in Libya would serve sufficiently important national interests to permit the President's action as Commander in Chief and Chief Executive and pursuant to his authority to conduct U.S. foreign relations").

136. *See* Memorandum from Timothy E. Flanigan, Assistant Attorney Gen., on Authority to Use United States Military Forces in Somalia to the Attorney Gen. (Dec. 4, 1992), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/10/Memorandum-from-Timothy-E.-Flanigan-Assistant-Attorney-Gen.-to-the-Attorney-General-"Memorandum-Opinion-for-the-Attorney-General"-Dec.-4-19921.pdf (denoting the protection of American citizens and American property as a justification for the use of force by the President).

137. *See* Krass, *supra* note 127, at 10 (denoting two national interest—preserving regional stability and supporting the United Nations Security Council's credibility and effectiveness—as a justification for the use of force by the President).

138. *See id.* at 18 (following Supreme Court precedent, the President's legal authority to use military force in Libya turned second on "whether the military operations that the President anticipated ordering would be sufficiently extensive in 'nature, scope, and duration' to constitute a 'war' requiring prior specific congressional approval under the Declaration of War Clause").

139. *See id.* at 13 (applying the analysis to determine whether limited airstrikes and associated support missions in Libya were within President Obama's legal authority).

iii. Covert Action and Reporting Procedures

Covert operations offer an alternate avenue for the President to assert limited war powers.[140] Covert action is defined as "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[141] The Executive may initiate these clandestine operations, via a presidential finding, so long as designated members of Congress are informed of the action prior to its launch or, under extenuating circumstance, within a timely fashion.[142] However, the President may not utilize covert action authority to conduct "traditional diplomatic or military activities."[143] Rather, military participation in covert operations must be limited to secretive missions "not under the direction and control of a military commander."[144]

B. *Presidential Initiatives to Make Cyber War*

President Obama has ordered the creation of USCYBERCOM,[145] conducted at least one known cyberwar operation,[146] and authored PPD-20 to assert executive authority in the realm of cyber warfare.[147] While the existence of these activities is known, many of the details remain classified. However, the intentions of the Obama administration can be inferred from the public record.

In 2009, President Obama authorized the use of a cyberweapon to attack the Iranian nuclear facility at Natanz.[148] The weapon, a virus later named Stuxnet, covertly interrupted the oscillation pattern of nuclear

140. BRADLEY & GOLDSMITH, *supra* note 47, at 274.

141. 50 U.S.C. § 413b(e) (2006).

142. *See* BRADLEY & GOLDSMITH, *supra* note 47, at 288 (outlining two exceptions to the President's duty to report covert actions).

143. § 413b(e)(2).

144. BRADLEY & GOLDSMITH, *supra* note 47, at 290.

145. *See* Obama, *supra* note 1 (announcing the creation of a new office at the White House to be led by the Cybersecurity Coordinator in a White House press release on May 29, 2009).

146. David E. Sanger, *Obama Order Sped Up Wave of Cyber Attacks Against Iran*, N.Y. TIMES (Jun. 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0 (discussing the "increasingly sophisticated attacks on the computer system that run Iran's main nuclear enrichment facilities").

147. *See generally* PRESIDENTIAL POLICY DIRECTIVE/PPD–20, *supra* note 17 (enumerating the cyber warfare policy for the United States).

148. Sanger, *supra* note 146. Early in his presidency, President Obama covertly initiated "increasingly sophisticated" attacks against Iranian computer systems at nuclear enrichment facilities, "significantly expanding" the use of cyberweapons. *Id.*

centrifuges, while allowing for a normal display on computer monitors.[149] It is difficult to report the exact damage caused by the Stuxnet virus, because Iran is understandably unwilling to share that information, but, some accounts from within the Obama administration claim the infrastructure damage was bad enough to set the Iranian nuclear program back eighteen to twenty-four months.[150]

It is difficult to determine whether the Obama administration classified Stuxnet as a military or intelligence operation, because the U.S. Government has not formally recognized the project. Rather, the United States has only accepted responsibility via leaked reports to *The New York Times*.[151] However, in a June 2012 article in *Congressional Quarterly*, Senator Carl Levin stated the Senate Select Committee on Intelligence and not the Armed Services Committee was briefed on the Stuxnet virus.[152] Thus, it can be inferred the Obama administration treated the offensive operation in Iran as a covert operation and not military action.[153] Regardless of the classification of the operation or the actual amount of damage inflicted upon Iran, the United States "crossed a Rubicon in cyberspace" when the President authorized the launch of the Stuxnet virus.[154] It appears—for the first time—the United States invaded the sovereignty of a foreign state with a cyberweapon to destroy critical infrastructure.[155]

More recently, in late 2012, President Obama issued PPD-20 to define the cyber war authority of the Executive.[156] This classified directive—one of the documents leaked to the public by Snowden[157]—reserves pres-

149. *See* CLARKE & KNAKE, *supra* note 28, at 295 (explaining how the Stuxnet virus damaged computers at the Natanz, Iran nuclear facility).

150. Sanger, *supra* note 146.

151. *See generally id.* (reporting on President Obama's decision to attack the Iranian nuclear facility with a cyberweapon and the aftermath of the cyberassault).

152. *See* Tim Starks, *Sorting Out Rules of Cyber War*, CONGRESSIONAL QUARTERLY (June 16, 2012, 1:05PM), http://public.cq.com/docs/weeklyreport/weeklyreport-000004107497.html ("Levin says he was not briefed about [Stuxnet] but that he believes the leaders of the Intelligence panels were.").

153. *See id.* ("The vice chairman of the Senate Select Intelligence Committee, Georgia Republican Saxby Chambliss, would only say: 'We are briefed on a good deal of what happens in cyber.'").

154. CLARKE & KNAKE, *supra* note 28, at 296.

155. *See generally* CLARKE & KNAKE, *supra* note 28, at 296 (discussing the history, impact, and potential ramifications of President Obama's novel decision to deploy the Stuxnet virus and thereby legitimize cyber warfare).

156. Presidential Policy Directive 20, U.S. CYBER OPERATIONS POLICY (Oct. 16, 2012), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

157. *See generally* Greenwald et. al., *supra* note 13.

idential power to conduct defensive and offensive cyber operations.[158] Even though historical and legal precedent would only allow the President to deploy the extraordinarily destructive potential of cyber power to protect traditional national interests from an actual or imminent harm or as the result of congressional approval, PPD-20 provides the President with a more expansive authority to initiate cyber attacks.[159]

The Obama Administration has yet to release a "red line" imminence test to clarify when a foreign nation's cyber operations rise to the level of imminent attack, thereby justifying defensive maneuvers by the President.[160] However, John O. Brennan, the author of the administration's policy on drone strikes, was also the thought-leader behind PPD-20.[161] Thus, one may assume the standard for an imminent attack in PPD-20 is similar to the analysis detailed in the white paper on drones.[162] If this is the case, then no clear evidence of a specific attack is required to trigger the self-defense powers of the Executive Branch.[163] Instead, a situation-specific analysis is to be applied, considering the "window of opportunity" for stopping an attack, the "possibility of reducing collateral damage to civilians, and the likelihood of heading off future disastrous attacks on Americans."[164]

Similarly, to initiate an offensive cyber attack, the President needs only to act in furtherance of "national objectives around the world."[165] National objectives include "matters of vital interest to the United States to include national security, public safety, national economic security, the safe and reliable function of 'critical infrastructure,' and the availability of

158. *See generally* Presidential Policy Directive 20, U.S. CYBER OPERATIONS POLICY (enumerating the cyber warfare policy for the United States).

159. *See id.* (asserting that "[Offensive Cyber Effects Operations] can offer unique and unconventional capabilities to advance U.S. national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging").

160. *See generally* Sanger & Shanker, *Broad Powers Seen for Obama in Cyberstrikes*, *supra* note 16 (reporting that "[a] secret legal review on America's growing arsenal of cyberweapons has concluded that President Obama has the broad power to order a preemptive strike if the United States detects credible evidence of a major digital attack looming from abroad").

161. *Id.*

162. *See generally* Memorandum from Department of Justice, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qa'ida or An Associated Force 7 (2013), *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf.

163. *See id.* (clarifying the imminent danger requirement necessary to initiate a drone strike).

164. *Id.*

165. Presidential Policy Directive 20, U.S. CYBER OPERATIONS POLICY, 9 (Oct. 16, 2012), *available at* https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf.

'key resources.'"[166] This vague rationale for action provides the President near universal justification to initiate offensive cyber operations.

Finally, during the creation of USCYBERCOM, which consolidated the cyber capabilities of all four military branches under one central command, President Obama appointed General Keith B. Alexander, the Director of the NSA, to serve simultaneously as the Commander of USCYBERCOM.[167] At the recommendation of Secretary of Defense Robert M. Gates, President Obama created this "dual-hatted position" in order to more effectively accomplish the mission of both organizations.[168] However, this leadership structure can also allow the President to evade checks on his power by blurring the traditional lines between intelligence and military activities and more freely classifying cyber military operations as covert action and vice versa. Nonetheless, despite calls to bifurcate the NSA and USCYBERCOM leadership, President Obama pledged to keep U.S. cyber intelligence and warfare activities under the same umbrella when he appoints General Alexander's replacement in 2014.[169]

V. LEGISLATIVE AUTHORITY TO REGULATE EXECUTIVE ACTION

A. *Constitutionally-Created Checks on the Executive*

The power to "raise and support" the military[170] is a powerful tool for Congress to check the war-making authority of the President,[171] because executive command of the military is limited to the operational capacity funded by congressional appropriations.[172] Additionally, Congress can attach restraints and reporting requirements to authorizations and appro-

166. *Id.*

167. David E. Sanger & Thom Shanker, *Obama to Keep Security Agency and Cyberwarfare Under a Single Commander* (Dec. 13, 2013), http://www.nytimes.com/2013/12/14/us/politics/obama-to-keep-security-agency-and-cyberwarfare-under-a-single-commander.html.

168. *See id.* (quoting Caitlin Hayden, spokeswoman for the National Security Council).

169. *Id.*

170. U.S. CONST. art I, § 8, cl. 12.

171. *See generally* Mackubin Owens, *Essays on Article I: Army Clause, The Heritage Guide to the Constitution*, THE HERITAGE FOUND., http://www.heritage.org/constitution#!/articles/1/essays/52/army-clause (last visited June 12, 2014) (explaining the intent of the founders' was to grant Congress the authority to control the existence and continual financing of a standing military as a check on the power of the Executive Branch).

172. *See* Yoo & Ho, *supra* note 51 ("[T]he President may be Commander in Chief, but he had nothing to command except what Congress may provide.").

priations to ensure executive compliance with congressional standards and oversight.[173]

B. *The War Powers Resolution*

In response to the Vietnam War, Congress passed the War Powers Resolution, over President Nixon's veto, to "fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities."[174] The Resolution limits the authority of the President to introduce the U.S. military into "hostilities" to occasions where (1) Congress has issued a declaration of war, (2) Congress has specifically authorized statutory authority for military engagement, or (3) a national emergency.[175] Furthermore, if the President has committed troops to hostilities, but no declaration of war has been granted, then the Executive is required to comply with initial and continuous reporting requirements to Congress.[176] The President must terminate military action sixty days after the initial report is filed, unless Congress has declared war, authorized the use of force, granted a sixty-day extension, or is physically unable to meet.[177]

C. *Congressional Limitations on Covert Action*

In a similar fashion, Congress also passed legislation in the aftermath of the Iran–Contra scandal to increase congressional oversight of covert actions.[178] As a result, the President is compelled to "keep the congressional intelligence committees fully and currently informed of all covert actions."[179] This requires the Executive to file presidential findings with each committee to confirm the legality of such operations.[180] However, the Executive may limit the audience for a finding to a group of eight

---

173. *See* ROLLINS & HENNING, *supra* note 26, at 16 (discussing congressional capabilities to regulate Executive Branch authority to operate a cyber military arsenal).

174. 50 U.S.C. § 1541(a) (2006).

175. § 1541(c).

176. § 1543(a).

177. § 1544(b).

178. *See* BRADLEY & GOLDSMITH, *supra* note 47, at 274–80 (discussing the history of the creation and evolution of covert action and the accompanying reporting requirements which are incorporated as part of the Commander-in-Chief's national security apparatus).

179. § 413b(b)(1).

180. *See* § 413b(a) (detailing the necessity and process for presidential findings regarding covert action).

critical representatives if the President determines limited access is essential for a specific covert action.[181]

D. *Executive Mitigation of Legislative Restraints*

On the other hand, the Executive is not rendered powerless by the aforementioned legislative restraints on presidential authority. Instead, the President can employ measures to counteract the limitations applied by Congress. First, each year the President is required to submit a detailed budget request to Congress for the following fiscal year.[182] This comprehensive plan allows the President to suggest to Congress how discretionary funds should be utilized in the upcoming year.[183] The President's budget also recommends funding levels for each discretionary government program.[184] Thus, the President is allowed to proclaim—to Congress and the public—his proposal for the requisite funding of the U.S. military.[185]

Second, each president since the passage of the War Powers Resolution has characterized the Resolution as an unconstitutional limitation on executive authority.[186] During this time, presidents have utilized the U.S. military in sixteen significant engagements and scores of minor operations.[187] Only three of these operations were "baptized" by Congress.[188] Therefore, in all other situations the "presidents justified their actions—in whole or in part—under the Commander in Chief and related presidential powers."[189] Presidents of both parties have continuously ignored the War Powers Resolution, or merely taken notice of it and submitted documentation "consistent with" the Resolution.[190]

---

181. § 413b(c)(2). The congressional "Gang of Eight" may be restricted by the President to "chairman and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, the majority and minority leaders of the Senate, and such other member or members of the congressional leadership as may be included by the President." *Id.*

182. Robert Langley, *About the President's Annual Budget Request, U.S. Government Info*, ABOUT.COM, http://usgovinfo.about.com/od/federalbudgetprocess/a/budgetprop.htm (last visited June 12, 2014).

183. *Id.*

184. *Id.*

185. *Id.*

186. ROLLINS & HENNING, *supra* note 26, at 15.

187. BRADLEY & GOLDSMITH, *supra* note 47, at 268–69.

188. *Id.*

189. *Id.* at 269.

190. *See* ROLLINS & HENNING, *supra* note 26, at 15 (citing RICHARD F. GRIMMETT, CONG RESEARCH SERV., RL33532, WAR POWERS RESOLUTION: PRESIDENTIAL COMPLIANCE (2012) for more information on presidential actions in accordance with the War Power Resolution).

Additionally, the Executive Branch has consistently utilized the statutory language of the Resolution to circumvent congressional authority.[191] For example, the Clinton Administration argued the specific appropriation of funds for a military operation was tantamount to a congressional authorization for the continuation of military activities after the sixty-day deadline imposed by the Resolution.[192] More recently, the Obama Administration declared a limited military engagement, as determined by an examination of the mission, exposure of forces, risk of escalation, and required military means, could be exempted from the Resolution's sixty-day withdrawal provision, because it does not rise to the level of "hostilities" envisioned by the Resolution's drafters.[193]

Finally, the Executive may order the Department of Defense to classify covert operations by the military as "operational preparation of the environment," instead of intelligence activities.[194] This classification allows the President to circumvent the reporting requirements of covert action, because the operation is subject to the jurisdiction of the House and Senate Armed Services Committees rather than the Intelligence Committees.[195] The reporting requirements for the former are less rigorous than those of the latter.[196]

VI. Cyber War and the Separation of Powers

A. *The Youngstown Sheet & Tube Co. Test*

As discussed in previous sections, the Legislative and Executive Branches possess independent and concurrent powers related to the U.S. military and war. As a result, the President, and to a lesser extent Congress, have attempted to mold the developing field of cyber warfare. However, the ultimate balance of power for cyber war is best examined through application of the test formulated by Justice Robert Jackson in his concurring opinion to *Youngstown Sheet & Tube Co. v. Sawyer.*[197]

---

191. *See* Bradley & Goldsmith, *supra* note 47, at 259–64 (exploring Executive Branch attempts in the Clinton and Obama Administrations to circumvent the congressional restrictions imposed by the War Powers Resolution).

192. *Id.* at 259–62.

193. *Id.* at 262–64.

194. Dycus, *supra* note 71, at 161.

195. *Id.*

196. *See id.* at 161, n.42 (implying that the congressional defense committees do not scrutinize operations in the same manner as intelligence committees).

197. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) (Jackson, J., concurring); *see* Rollins & Henning, *supra* note 26, at 11 (analyzing the *Steel Seizure Cases* and the usefulness of Justice Jackson's concurring opinion for determining the extent of presidential authority to make war).

Also referred to as "*The Steel Seizure Case*," *Youngstown Sheet & Tube Co.* considered the ability of the President to unilaterally assert Executive control over private industry in the name of national security.[198] President Truman claimed the Commander-in-Chief clause afforded him the power to take control of the steel industry to prevent a strike, because steel production was essential to support the military action in Korea.[199] The Supreme Court rejected this assertion of executive authority.[200]

In a famous concurring opinion, Justice Jackson reasoned the inherent constitutional powers of the Executive "fluctuate" from high to low depending upon their relationship to actions taken by Congress.[201] When the President acts in a manner authorized by Congress, executive power is at its zenith; but when the Executive "takes measures incompatible with the express or implied will of Congress" presidential power is at its "lowest ebb."[202] Thus, Justice Jackson outlined three zones of executive action: "(1) action supported by an express or implied grant of authority from Congress; (2) a 'zone of twilight' between the other categories, in which 'congressional inertia' can occasionally 'enable, if not invite, measures on independent presidential responsibility'; and (3) action that conflicts with statutes or congressional intent."[203]

B. *Zone One: The Zenith of Executive Authority*

Presidential acts in response to a congressional grant of power represent the apex of executive authority because the President does not have to rely solely on inherent Article II powers.[204] Therefore, if Congress authorizes presidential action by legislation, pursuant to the enumerated powers of Article I, the President possesses full authority to execute the mission, as detailed by statute.[205]

---

198. *See generally Youngstown*, 343 U.S. 579 (limiting the ability of President Truman to use his Commander-in-Chief powers during the Korean War to forestall a steel industry strike in the name of national defense).

199. *Id.* at 582, 678.

200. *Id.* at 587–89.

201. *Id.* at 635–38 (Jackson, J., concurring).

202. *Id.* at 637 (Jackson, J., concurring).

203. ROLLINS & HENNING, *supra* note 26, at 12.

204. *See Youngstown*, 343 U.S. at 635–38 (Jackson, J., concurring) (stating that presidential power is at its highest when acting as the result of a congressional act; at its lowest when acting counter to a congressional act; and somewhere in between when Congress is silent).

205. *See id.* at 635–37 (Jackson, J., concurring) (stating that "[w]hen the president acts pursuant to an express or implied authorization of Congress, his authority . . . includes all that he possesses on his own plus all that Congress can delegate" and that the only reason his action could be held unconstitutional is if "Federal Government as an undivided whole lacks power" to carry out the action).

In NDAA-FY12, Congress statutorily recognized the ability of the President to conduct offensive military operations in cyberspace.[206] NDAA-FY13 re-affirmed the offensive capabilities of the President and formally recognized the executive authority to initiate defensive cyber action.[207] Thus, NDAA-FY12 and NDAA-FY13 afford the President statutory authorization to conduct offensive and defensive cyber warfare.[208] The only constraints placed on executive authority are those explicitly stated in NDAA-FY12.[209] However, the President must also refrain from violating other provisions of the Constitution.[210] As a result, the powers President Obama reserved for the Executive in PPD-20 are supported by the zenith of executive authority.

C. *Zone Two: The Twilight Zone*

The second zone of Justice Jackson's analysis governs situations where presidential and congressional authorities overlap.[211] A subsequent Supreme Court case, *Dames & Moore v. Regan,*[212] articulated the necessary separation-of-powers evaluation for cases that fall within this zone of twilight.[213] In *Dames*, the Court said the analysis "hinges on a consideration of all the circumstances which might shed light on the views of the legislative branch toward [the Executive's] action, including 'congressional inertia, indifference or quiescence.'"[214] Thus, congressional interest in the issue must be measured and weighed against executive action.

---

206. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

207. *See* National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 940, 126 Stat. 1632, 1888–89 (2012) (reaffirming the congressional recognition of presidential power to conduct offensive cyber warfare).

208. *See Youngstown*, 343 U.S. at 635–37 (Jackson, J., concurring) (explaining that even when the President is given power that has been authorized Congress he must act within the confines of what the Constitution allows or the President's actions may be found to be unconstitutional).

209. *See* National Defense Authorization Act for Fiscal Year 2012 § 954, 125 Stat. at 1551 ("upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, *subject to—(1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and (2) the War Powers Resolution*) (emphasis added).

210. *See Youngstown*, 343 U.S. at 635–37 (Jackson, J., concurring) (stating that "[w]hen the president acts pursuant to an express or implied authorization of Congress, his authority . . . includes all that he possesses on his own plus all that Congress can delegate" and that the only reason his action could be held unconstitutional is if "Federal Government as an undivided whole lacks power" to carry out the action).

211. ROLLINS & HENNING, *supra* note 26, at 12.

212. Dames & Moore v. Regan, 453 U.S. 654 (1981).

213. ROLLINS & HENNING, *supra* note 26, at 13.

214. *Dames & Moore*, 453 U.S. at 668–69.

The statutory language of NDAA-FY12 and NDAA-FY13 recognized executive authority and placed two separate restraints on cyberwarfare.[215] Any other issues, where the statutes are silent, fall within this twilight zone of power.[216] Therefore, "congressional inertia, indifference or quiescence" must be determined to ascertain the breadth of executive authority.[217]

The Bush Administration first addressed cyber war with the Comprehensive National Cyber Initiative of 2008.[218] Since then Congress has continually appropriated funds for military and covert operations focused on cyberspace.[219] Therefore, legislative momentum, as seen through authorizations and appropriations, favors unilateral executive authority. Moreover, Congress stood idly by as President Obama created USCYBERCOM, launched the Stuxnet virus attack on Iran, and issued PPD-20. Thus, legislative acceptance of executive authority and an apathetic approach to oversight may be inferred from congressional silence, outside of the aforementioned acts.

D. *Zone Three: The "Lowest Ebb" of Executive Authority*

The President's authority is at its lowest level when executive action exceeds legislative boundaries, because the President is forced to retreat solely to the vested powers of Article II.[220] Thus, the President's author-

---

215. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) ("upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, *subject to*—(1) *the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and* (2) *the War Powers Resolution*) (emphasis added).

216. *Dames & Moore*, 453 U.S. at 668 (stating "[w]hen the President acts in the absence of congressional authorization he man enter 'a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain'").

217. *Id.* at 668–69.

218. *See generally* ROLLINS & HENNING, *supra* note 26 ("The [Comprehensive National Cybersecurity Initiative] establishes a multipronged approach the federal government is to take in identifying current and emerging cyber threats, shoring up current and future telecommunications and cyber vulnerabilities, and responding to or proactively addressing entities that wish to steal or manipulate protected data on secure federal systems.").

219. *See* Michaels, *supra* note 92 (detailing the use of funds given by Congress to the Department of Defense for cyber warfare operations).

220. *See* ROLLINS & HENNING, *supra* note 26, at 13 (remarking that "at least some actions contemplated by the CNCI likely fall outside of the relatively straightforward and narrow delegations of authority granted by statutes that specifically address cybersecurity[,]" and where Congress declines to act legislatively "the Executive Branch could act in a number of situations by relying on inherent powers under Article II of the U.S. Constitution or, in very limited circumstances on the 2001 Authorization to Use Military Force").

ity drops precipitously if executive action is counter to or exceeds these boundaries.[221]

According to NDAA-FY12, cyber operations are restricted by the same legal parameters as kinetic warfare and are subjected to the strictures of the War Powers Resolution.[222] Consequently, the use of forces outside of these parameters would require the President to rely on Chief Executive and Commander-in-Chief powers to initiate cyber war activities.[223] For example, the President would need to couch the utilization of cyber force in an act of self-defense or a mission to protect national interests. The latter would also require the President to establish that the nature, scope, and duration of the cyber mission precludes the need for congressional authorization, and is such that it is outside the realm of "hostilities" addressed by the War Powers Resolution.[224] Otherwise, the President is forced to act upon power that can be checked or overridden by the constitutional and statutory power of Congress.[225]

VII. Civil Liberties and Unilateral Executive Authority to Conduct Cyber Warfare

Much like traditional, kinetic warfare, cyber war can be devastating to the infrastructure, economy, and health and safety of a civilian population.[226] However, unlike other types of war, the weaponry and machinations of cyber war are largely invisible. Thus, lack of perceptibility and the general sense of detachment citizens feel from cyber-related activities could allow for the U.S. Government, at the sole direction of the President, to prepare for and engage in a perpetual state of cyber war. This constant state of war not only presents a threat to the welfare of Ameri-

221. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 638(1952) (Jackson, J., concurring) (pointing out that if a President were able to act outside of his power and those not given to him by Congress, "the equilibrium established by or constitutional system" would be at stake).

222. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011).

223. *See Youngstown*, 343 U.S. at 635–37 (Jackson, J., concurring) (explaining that "[w]hen the President takes measures incompatible with the expressed or implied will of Congress . . . he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter.").

224. *See* 50 U.S.C. § 1541(c) (2006) (indicating the three situations where the President as Commander-in-Chief may commit U.S. armed forces to hostilities); *see also* § 1543(a) (explaining what the President must report to Congress if U.S. armed forces are introduced to hostilities without a declaration of war).

225. *See* § 1544(b) (stating that the President must terminate any use of the U.S. armed forces within sixty days unless Congress allows one of the three exceptions listed).

226. Sanger, *supra* note 146 (implying that the U.S. cyberattack on Iran using the Stuxnet virus caused a lot of damage to infrastructure and the economy of Iran).

can citizens; but if history is any judge, it will most likely lead to the degradation and erosion of civil liberties.

Throughout American history the United States has traditionally restricted civil liberties and attempted to punish citizens for dissent in times of war.[227] In 1798, with the nation nearing war with France, Congress passed the Sedition Act, which made it illegal to speak ill of the government, Congress, or the President.[228] "[D]uring the Civil War, President Lincoln suspended the writ of habeas corpus" and many of his critics were imprisoned.[229] Opposition to the war or the draft was again punishable by imprisonment during World War I, and dissent or Japanese heritage were unfortunately enough to justify deportation or internment during World War II.[230] The Cold War wrought mandatory loyalty programs, congressional investigations into the lives of citizens, and criminal prosecutions for membership in communist organizations.[231] Citizens and media outlets alike were stifled and punished for participating in and covering dissident political activities during the Vietnam War.[232] And, most recently, numerous intrusive intelligence measures, including the NSA programs leaked by Edward Snowden,[233] and even a drone strike against an American citizen,[234] were utilized in furtherance of the battle against terrorism.

Therefore, this danger of diminishing civil liberties must be omnipresent in the minds of citizens, Congress, and the President as the United States enters the invisible and sure to be recurring world of cyber war. As long as the President can unilaterally thrust the nation into a cyber war without meaningful debate or legislative regulations, the citizens of the United States are merely a click of the mouse away from having their civil liberties curtailed in favor of unfettered support for the government in the name of national security.

---

227. *See* GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME—FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 12 (2004) (discussing the history of civil liberty restrictions imposed by the U.S. Government during the undeclared war with France, the Civil War, World War I, World War II, the Cold War, and the Vietnam War).

228. *Id.*

229. *Id.*

230. *Id.*

231. *Id.* at 12–13.

232. *Id.* at 13.

233. *See generally The NSA Files*, THE GUARDIAN, http://www.theguardian.com/world/the-nsa-files (last visited Sept. 20, 2014).

234. Spencer Ackerman, *US cited controversial law in decision to kill American citizen by drone*, THE GUARDIAN (Jun. 23, 2014), http://www.theguardian.com/world/2014/jun/23/us-justification-drone-killing-american-citizen-awlaki (stating the US government cited an anti-terrorism law in its justification for killing an American citizen with a drone attack).

VIII. Conclusions and Recommendations

Shortly after his inauguration, President Obama approved the first cyber act of war the world had ever seen.[235] The Stuxnet virus was deployed to destroy critical infrastructure in Iran, but along the way it changed the course of modern warfare.[236] The United States had legitimized cyber war.

In preparation for this new realm of conflict, the President has developed new strategies, implemented policies, and made organizational changes to prepare the U.S. military for cyber war. Congress, on the other hand, has been slower to act. Congress has recognized the offensive and defensive cyber capabilities of the Executive Branch, but it has done little to regulate this authority. Instead, Congress has halfheartedly applied conventional warfare principles to an unconventional type of combat.

Important restrictions on executive war-making authority remain unaddressed. For example, how does the "imminent threat" trigger of self-defense relate to cyber attacks that can occur in a matter of seconds? PPD-20 affords the President the authority to initiate offensive cyber action in the name of U.S. national interests. How are these national interests defined and to what extent may the President act without first conferring with Congress? In NDAA-FY12, Congress declared cyber war attacks are subject to the War Powers Resolution. But, how is an act of war that requires no troops on the ground, eschews traditional weaponry, and occurs at the speed of light, measured within a War Powers Resolution analysis? Furthermore, no structures are in place to distinguish between cyber military operation and covert cyber action. Thus, there is nothing to stop the President from playing a shell game with cyber operations to avoid congressional oversight and the requirement for an authorization of force. Currently, President Obama, and his national security team, classify all cyber attacks as clandestine and refuse to acknowledge their existence or use.[237]

As a result, cyber warfare is essentially an "open field" for the President to assert executive authority. Therefore, Congress must legislate limitations on the President to prevent this unconventional, yet powerful

---

235. Sanger, *supra* note 146.

236. *See* Clarke & Knake, *supra* note 28, at 295 (explaining how the Stuxnet virus damaged computers at the Natanz, Iran nuclear facility).

237. Barton Gellman & Ellen Nakashima, *U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show*, Wash. Post (Aug. 30, 2013), *available at* http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html.

method of war from becoming an unchecked tool of the Executive. However, at the same time, Congress must be careful not to statutorily handcuff the President from adapting cyber war strategies and rules of engagement to meet the ever-evolving cyber battlefield. Thus, Congress should implement a few specific statutory limitations on the Executive, and utilize appropriations to assert oversight capabilities and shape the parameters of cyber war.

As such, Congress should consider the following recommendations. First, Congress should initiate legislation to develop a statutory definition of cyber war. This definition should be flexible enough to account for changes in technology, but it should also demarcate the point at which presidential action must yield to congressional authorization. Congress should then initiate legislation to differentiate between cyberwar operations and covert action. This distinction will determine the type of reporting requirements with which the President must comply for a cyber mission.

Second, Congress should establish House and Senate sub-committees of the Armed Services Committee specifically dedicated to cyber warfare. Additionally, oversight restrictions for cyber military operations should be tied to future defense appropriations. This will prevent the President from hiding cyber operations under the guise of covert action and thereby eschewing meaningful congressional reporting requirements. Cyber warfare employs non-traditional weaponry, but it is still a form of military combat. Thus, the President's use of cyberweapons should be held to the same accountability standards as those for the use of missiles, bombs, and bullets.

Third, Congress should require the President to provide the necessary committees with definition for imminent threat and the advancement of national interests, for the purposes of cyber war. However, this information should remain classified to prevent foreign nations from discovering the United States' threshold for the implementation of defensive and offensive cyber operations.

Fourth, Congress should amend the War Powers Resolution to account for cyber war operations, or exclude cyberwar from the Resolution. If Congress chooses the latter, it should author similar legislation to limit the ability of the President to commit the United States to a cyber war that could escalate quickly and last perpetually. Similarly, Congress should host hearings and make recommendations to the President on the applicability of conventional warfare principles, policies, and legal regimes to cyber war.

Finally, Congress should host hearings and make a recommendation to the President regarding the commingling of leadership and funds at US-CYBERCOM and the NSA. President Obama is resolute in his belief a

single commander, and not separate leaders, should replace General Alexander as the boss of the NSA and USCYBERCOM. An outside advisory panel recently suggested otherwise, in the name of better civil liberty protection, but the President remains undeterred.[238] Thus, Congress should bring in military strategy experts, intelligence officials, and representatives from civil liberty organizations to determine the most efficient yet protective leadership structure for the cyber intelligence and warfare apparatus.

238. Sanger & Shanker, *supra* note 167.