Michigan Law Review

Volume 111 | Issue 3

2012

Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations

Aaron P. Brecher
University of Michigan Law School

NOTE

CYBERATTACKS AND THE COVERT ACTION STATUTE: TOWARD A DOMESTIC LEGAL FRAMEWORK FOR OFFENSIVE CYBEROPERATIONS

*Aaron P. Brecher**

Cyberattacks are capable of penetrating and disabling vital national infrastructure, causing catastrophic economic harms, and approximating the effects of war, all from remote locations and without the use of conventional weapons. They can be nearly impossible to attribute definitively to their sources and require relatively few resources to launch. The United States is vulnerable to cyberattacks but also uniquely capable of carrying out cyberattacks of its own. To do so effectively, the United States requires a legal regime that is well suited to cyberattacks' unique attributes and that preserves executive discretion while inducing the executive branch to coordinate with Congress. The trouble is that it is unclear which domestic legal framework should govern these attacks. The military and intelligence communities have disputed which of their respective legal regimes should control. The choice between these frameworks raises important issues about the policy benefits of the executive branch keeping Congress informed regarding cyberattacks that it conducts. It also raises constitutional questions about the branches' respective roles in warmaking when the chosen course of conduct blurs the line between an intelligence operation and an act of war. This Note argues that, in the absence of an independent congressional authorization to use force against a target, the covert action statute, which demands written reports from the president to the congressional intelligence committees in advance of operations, should presumptively govern, and that the president should issue an executive order to that effect.

TABLE OF CONTENTS

* J.D. Candidate, May 2013, University of Michigan Law School. I am grateful to all of the editors of the *Michigan Law Review*, especially Becca Klein, Hannah Miller, and Allison Nichols, for shepherding this Note to publication. For helpful comments throughout the writing process, I thank Professor Julian Davis Mortenson; his generosity was matched only by his depth of knowledge in this field. Finally, my greatest thanks must go to my family, especially my wife Carolyn, whose love and support made this project possible before it even began.

INTRODUCTION

In the second half of 2009, a serious computer virus began working its way through Iranian computer systems, eventually reaching the Natanz nuclear enrichment facility, where it damaged many hundreds of centrifuges used to produce enriched uranium.[1] The virus, known as Stuxnet, was designed to target specific industrial control processes and appears to have been aimed specifically at the Natanz enrichment facility.[2] The damage from Stuxnet was so extensive that the facility had to be shut down briefly.[3] Though the source of Stuxnet is not known definitively, press reports suggest that the United States created the virus with assistance from Israel.[4]

The Stuxnet incident highlights the increasing importance of cybersecurity as a key aspect of national security. It shows that sophisticated software that is difficult to attribute definitively to its source can cause tangible damage beyond cyberspace—potentially enough damage to be considered an act of war. U.S. policymakers have considered the possible courses of action that could be adopted in a cyberwar, and in 2011, the Pentagon announced that it might respond to certain cyberattacks on critical U.S. infrastructure with counterstrikes using conventional weapons.[5] Much of the public debate

1. Joby Warrick, *Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyberattack*, WASH. POST, Feb. 16, 2011, at A01.

2. *Id.*

3. *Id.*

4. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (describing Stuxnet as part of a larger campaign of cyberattacks against Iran carried out by U.S. intelligence and military officials, with aid from Israeli officials).

5. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, at A1.

on cybersecurity has focused on how to *prevent* cyberattacks.[6] This Note analyzes the domestic legal regime that should govern the use of cyberattacks by the United States, especially outside the context of an otherwise traditional conflict.

The term "cyberattack," as used in this Note, refers to a "deliberate action[] to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information [or] programs resident in or transiting these systems or networks."[7] Key characteristics of cyberattacks include the great difficulty of attributing them definitively to their sources,[8] and their potential to cause almost instantaneous effects from anywhere in the world.[9] Cyberattacks are frequently confused with cyberexploitation, which as a technical matter is similar. The key difference is that cyberexploitation involves only the monitoring or copying of data, while cyberattacks involve the manipulation of data.[10] This Note discusses only the latter.

One lens through which to evaluate the proper domestic legal framework for cyberattacks is whether such operations should rely on intelligence legal authority (called "title 50" authority) or military legal authority (called "title 10" authority).[11] Under the military framework, the president is often free to order a wide range of operations without giving advance

---

6. *See* NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 10 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT]. The National Research Council ("NRC") Report contains the most valuable general discussion that I have seen of all aspects of cyberattack, including the legal implications of its use by the United States.

7. *Id.* at 1.

8. *See* PHILIP BOBBITT, TERROR AND CONSENT 96 (2008) ("There is still no technology for determining the source of a disguised cyberattack . . . ."); Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 24, 2010, at 21, 23 (reviewing RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR (2010)).

9. Goldsmith, *supra* note 8, at 23.

10. NRC REPORT, *supra* note 6, at 1–2; Goldsmith, *supra* note 8, at 22. A few examples may help illustrate this distinction. A cyberoperation that infiltrates the network of a country's foreign ministry and copies communications to and from embassy personnel would be a cyberexploitation. An infiltration that disrupts the network at a foreign weapons manufacturing facility would be a cyberattack. Such martial effects need not be present in a cyberattack, however. Manipulating data on electronic ballots in order to alter the results of a foreign election would also be a cyberattack, as would manipulating an email server into listing false senders for the communications that it displays.

11. The debate over whether the military's or the intelligence community's legal regimes should govern particular actions is frequently invoked in national security discussions. *See, e.g.*, Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 J. NAT'L SECURITY L. & POL'Y 539 (2012) [hereinafter Chesney, *Military-Intelligence Convergence*]; Jeffrey H. Smith, Symposium, *State Intelligence Gathering and International Law—Keynote Address*, 28 MICH. J. INT'L L. 543, 546–47 (2007) (arguing that executive branch lawyers often debate the question of which framework governs certain activities). This Note refers to "title 10" authorities as shorthand for military authorities because that is the language employed in much of the academic literature. However, some of the more important limitations on U.S. military authority are codified outside of title 10 of the United States Code. *See, e.g.*, Posse Comitatus Act, 18 U.S.C. § 1385 (2006); War Crimes Act of 1996, 18 U.S.C. § 2441; War Powers Resolution, 50 U.S.C. §§ 1541–1548 (2006).

notice to Congress.[12] However, under the intelligence regime, covert actions, which are "activities . . . to influence political, economic, or military conditions abroad, where it is intended that the role of the [U.S. government] will not be apparent or acknowledged publicly,"[13] require written findings by the president that the operation is important to U.S. national security and reports made to the congressional intelligence committees.[14] Many cyberattacks could conceivably be carried out under either military legal authority or intelligence legal authority. However, the choice of a presumptive legal regime for national security policies could have an important effect on strategy,[15] as well as profound implications for the accountability of the executive branch to Congress.[16]

Engaging with the issues surrounding cyberattacks is important in part because American dependence on networked communications in both the private and public spheres makes the United States extremely vulnerable to cyberattacks.[17] At the same time, the United States is also among the best-equipped countries in the world to carry out offensive cyberattacks of its own.[18] Having the proper legal framework to regulate America's offensive use of these powerful tools will prove increasingly important as cyberattacks emerge as attractive options for dealing with cyberthreats (and physical threats) posed by terrorist groups as well as dealing with individuals who have the ability to use this relatively inexpensive cyberattack system.[19]

This Note argues that the Intelligence Authorization Act for Fiscal Year 1991's definitions and regulations of covert action[20] (hereinafter the "covert action statute") should provide the presumptive legal framework for cyberattacks initiated by the U.S. government, especially when the operation may

---

12. Smith, *supra* note 11, at 546.

13. 50 U.S.C. § 413b(e).

14. *Id.* § 413b(a)–(d). For more detail on the reporting requirements, see *infra* Section I.A.1.

15. *See* PHILIP BOBBITT, THE SHIELD OF ACHILLES 5–10 (2002); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 424–25 (2011). Probably the most sophisticated elaboration of the deep relationship between law and strategy is Professor Bobbitt's. *See generally* BOBBITT, *supra*.

16. *See generally infra* Part III.

17. *See* CLARKE & KNAKE, *supra* note 8, at xiii ("[C]yber war places [the United States] at greater jeopardy than it does any other nation."); Goldsmith, *supra* note 8, at 24 (noting that over 90 percent of U.S. military and intelligence communications travel over privately owned telecommunications networks); *see also* BOBBITT, *supra* note 8, at 234 (calling a cyberattack on the U.S. financial infrastructure an event that could threaten the consensual basis of the American government's rule).

18. Jack Goldsmith, Op-Ed., *Can We Stop the Global Cyber Arms Race?*, WASH. POST, Feb. 1, 2010, at A17.

19. See NRC REPORT, *supra* note 6, at 273–77, on the danger posed by nonstate actors. See also Eric Schmitt & Thom Shanker, *U.S. Weighed Use of Cyberattacks to Weaken Libya*, N.Y. TIMES, Oct. 18, 2011, at A1, for a suggestion that uncertainty over the legal implications of cyberattacks contributed to a decision not to employ them in the Libya conflict.

20. Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, tit. VI, sec. 602(a)(2), § 503, 105 Stat. 429, 442–44 (1991) (codifed at 50 U.S.C. § 413b (2006)).

affect neutral parties or the target is not already the object of a congressional authorization to use force. Part I summarizes the competing intelligence and military legal regimes. It then argues that cyberattacks pose unique problems when carried out under the military framework because of the difficulty of attributing a cyberattack to its source and the possibility of an attack producing serious effects on persons and infrastructure in allied countries. It concludes that the intelligence (covert action) regime can properly govern a wider range of actions than the military regime. Part II contends that, for cyberattacks with warlike effects, the covert action statute might serve as an alternative domestic legal basis to a traditional authorization to use force. Part II also argues that there are constitutional advantages to executive–legislative coordination when it is uncertain whether an attack amounts to a use of force—the alternative source of statutory support strengthens the president's authority to act in ambiguous circumstances. Finally, Part III concludes that the covert action statute provides the best balance between executive independence and congressional oversight among the two existing legal frameworks. It advocates that the president issue an executive order making the covert action regime the presumptive procedure for conducting cyberattacks.

I. THE COVERT ACTION AND MILITARY REGIMES EXPLORED

It is first useful to delineate the detailed statutory requirements for carrying out covert actions, as well as the circumstances under which the military may engage in cyberattacks. To that end, Section I.A briefly summarizes the covert action and military regime procedures. Section I.B then argues that the unique features of cyberspace make applying the law of armed conflict very difficult. Specifically, uncertainty over which cyberattacks constitute a use of force under international law could hamper the military's legal ability to launch cyberattacks under the military authority regime. Section I.C argues that while the covert action framework is not a catchall for every cyberattack that the government may wish to initiate, it does provide a legal basis for a considerable range of offensive actions in cyberspace. Examining the definition of covert action and an important exception to this definition, Section I.C shows that the covert action framework can be used by any number of agencies operating under a single framework, and it adapts well to the increasing blending of military and intelligence functions in the American national security apparatus.

A. *Comparing the Covert Action and Military Regimes*

Both military and intelligence activities are subject to complex internal planning and approval procedures. The most relevant difference between the respective legal regimes for purposes of this Note is that covert actions require the president to submit written "findings" to Congress whereas "execute orders" lack similarly rigorous reporting requirements. A "finding" is a written report authorizing a covert action that the president must submit

to the relevant congressional committees in advance of the operation.[21] An "execute order" is the analogous source of authority for military operations, and can be issued by the president or other high-ranking military officials.[22]

1. The Covert Action Regime: Written Findings and Advance Reports to Congressional Intelligence Committees

The covert action statute establishes a norm of submitting ex ante written reports to congressional intelligence committees that describe an impending operation, as well as the national security interest that it will serve. The statute dates back to 1991[23] and was first enacted in response to the Iran–Contra affair.[24] A covert action is an activity designed to influence conditions abroad in situations where the U.S. role is not meant to be publicly acknowledged.[25] Importantly, the definition of covert action excludes, among other things, "traditional diplomatic or military activities or routine support to such activities."[26] It follows from this exclusion that even activities meant to be unacknowledged or potentially unacknowledged are not covert actions if they are traditional military activities.

Before initiating a covert action, the president must make a written finding that the action supports an identifiable foreign policy objective and is important to national security.[27] The finding must also specify each U.S. government "department, agency, or entity . . . authorized to fund or otherwise participate in any significant way" in the action.[28] "A finding may not authorize any action that would violate the Constitution or any statute . . . ."[29]

Normally, the finding must be submitted to the members of the congressional intelligence committees soon after the decision is made and before the action is initiated.[30] When the need for secrecy is very great, however, the president has the option of initially submitting the finding only to the Speaker and minority leader of the House, the majority and minority leaders of the Senate, and the chairmen and ranking members of the two intelligence committees.[31] If neither of these reporting procedures is followed, the

---

21. *See* 50 U.S.C. § 413b(a) (2006).

22. *See* Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 574.

23. Intelligence Authorization Act, Fiscal Year 1991, Pub. L. No. 102-88, tit. VI, sec. 602(a)(2), § 503, 105 Stat. 429, 442–44 (1991) (codified at 50 U.S.C. § 413b (2006)).

24. JAMES E. BAKER, IN THE COMMON DEFENSE 150 (2007).

25. 50 U.S.C. § 413b(e).

26. *Id.* § 413b(e)(2).

27. *Id.* § 413b(a). Where urgency does not permit an advance finding, a written record of the president's decision must be contemporaneously made and reduced to a written finding no more than forty-eight hours after the decision is made. *Id.* § 413b(a)(1).

28. *Id.* § 413b(a)(3).

29. *Id.* § 413b(a)(5).

30. *Id.* § 413b(c).

31. *Id.* § 413b(c)(2).

president must make a timely report to the committees, as well as give reasons for the delay.[32]

2. The Military Regime: Execute Orders and Limited Congressional Notification

Unlike covert actions, military operations do not require written findings. Instead, "execute orders" are the source of authority for initiating such actions.[33] These orders may state an obligation to seek approval from certain officials, even the president or secretary of defense, to conduct certain types of operations.[34] In addition, an execute order, unlike a finding, can function as an ex ante authorization to act if particular circumstances arise.[35] Thus, the orders can, but need not, substantially replicate an internal process similar to that for covert action.[36]

As for reporting to Congress, the president has an obligation under the War Powers Resolution to make a written report to the entire Congress within forty-eight hours of introducing U.S. military forces into active hostilities.[37] Notably, though, the Obama Administration has taken an extremely narrow view of what constitutes "hostilities," so that many military activities will likely not be reported under the War Powers Resolution.[38] While there are other statutes in place that require reports of certain military activities to the congressional armed services committees, there is nothing analogous to the covert action requirements, and many activities are exempt from any reporting requirements.[39]

In the case of cyberattacks in particular, a recently enacted statute seems to require additional procedures. The National Defense Authorization Act for Fiscal Year 2012, an annual appropriations bill that funds and governs the military, provides that the military may conduct offensive operations in

---

32. *Id.* § 413b(c)(3).

33. Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 574.

34. *Id.* at 605.

35. *See id.* at 606.

36. *See id.* at 605.

37. War Powers Resolution, 50 U.S.C. § 1543(a).

38. Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 612. Specifically, the Obama Administration has claimed that the strikes in Libya in summer 2011 did not amount to "hostilities" based on factors including the limited nature of the mission, the minimal direct exposure of U.S. armed forces to harm, the limited potential for escalation, and the limited military means used. *Libya and War Powers: Hearing Before the S. Comm. on Foreign Relations*, 112th Cong. 12–17 (2011) (statement of Harold Koh, Legal Adviser, U.S. Department of State). Applying these factors to cyberattacks, which do not require forces on the ground, it is difficult to conceive of a cyberattack that would trigger the provisions of the War Powers Resolution. *See* Robert Chesney, *Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate*, LAWFARE (Dec. 14, 2011, 10:17 PM) [hereinafter Chesney, *Offensive Cyberspace Operations*], http://www.lawfareblog.com/2011/12/cyberoperations/.

39. Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 612–13.

cyberspace, subject to presidential approval.[40] It does not appear that presidential approval is required for other cyberoperations that are not cyberattacks, such as cyberexploitations. Moreover, it is unclear whether the presidential-approval requirement means that each specific cyberattack must be approved, as is the case with covert action, or whether there can be an advance presidential authorization to conduct a cyberattack under certain conditions, like with other execute orders.

B. *The Military and Cyberattacks: An Uncomfortable Fit*

This Section argues that the legal regime generally governing military action is not always well suited to governing cyberattacks. Cyberattacks' key attributes—remote access, unpredictable effects, and difficulty of attribution—can result in fundamentally different legal problems than conventional weapons attacks. This is because many cyberattacks bear no similarity to military attacks at all. Those that arguably constitute a use of force under international law are even more problematic.

A military's essential purpose is national defense. When many think of military operations, they first imagine kinetic strikes: the use of bombs, guns, and other conventional weapons. The emergence of the cyberattack as a viable tool of warfare enables a military with sufficient technological capacity to disable an enemy's communication network, issue false orders, and even impair critical infrastructure, such as by shutting down a power grid, all without firing a shot or even entering the enemy's territory.[41] Although the United States has taken advantage of earlier advances in technology for strategic gain[42] without sustained confusion over the law that governs the use of those tools, activity in the digital world cannot always be neatly analogized to activity in the physical world.

Given that the term cyberattack denotes any action to alter, degrade, or destroy data on computer programs or networks,[43] it should be obvious that many cyberattacks bear no resemblance to warlike actions in their effects. For example, almost no one would label an attack that temporarily shuts down service on a private commercial website an act of war. In situations in which the United States has a legitimate national security interest in carrying out such an attack, it is unlikely that the military would play a helpful

---

40. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) (codified as note to 10 U.S.C. § 111 (Supp. V 2011)).

41. *See* Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SECURITY L. & POL'Y 63, 69–70 (2010).

42. Many commentators have analyzed the strategic impact of technological advances in the United States. *See* NRC REPORT, *supra* note 6, at 293–96 (analogizing cyberoperations to the development of nuclear weapons and nuclear strategy); Andrew F. Krepinevich, *Cavalry to Computer: The Pattern of Military Revolutions*, NAT'L INT., Fall 1994, at 30; *see also* MAX BOOT, WAR MADE NEW 268–436 (2006).

43. *See supra* text accompanying note 7.

role.[44] The more difficult analytical issues arise when the physical effects of a cyberattack are substantially similar to those of an armed attack under the terms of article 51 of the United Nations ("UN") Charter, which recognizes an inherent right of self-defense in the event of an armed attack on a UN member state.[45]

One test to determine whether cyberattacks constitute an armed attack or use of force depends on whether the real-world effects of the operations are equivalent to those of a traditional physical attack,[46] but this effects-based approach can be difficult to apply.[47] Once one shifts to the digital realm, with its features of remote access and relative anonymity, analogizing activities to those that take place in the physical world can be a frustrating exercise. One prominent analogy discussed in the cyberattack literature is the distinction between economic sanctions and a blockade.[48] Economic sanctions are not a use of force under international law.[49] But a blockade, which may have the same effect, is.[50] Unlike sanctions, a blockade involves physically stopping or threatening to physically stop shipments. Applying this analogy to cyberattacks, the debate centers on what type of economic impact might justify either a warlike cyberattack in response or an attack in the physical world. For example, it is unclear whether an attack that manipulates data on a stock exchange, causing a devastating economic impact, constitutes a use of force.[51] Similarly, is a cyberattack that targets a specific industry, in a similar manner to illegal blockades and legal sanctions, a use of force?[52]

---

44. This is not necessarily true if the skills to conduct such an attack are the same as those required for cyberwar. Still, such an attack seems to be outside the scope of the military's mission, unless the operation were in support of a larger military conflict.

45. U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations . . . ."). Importantly, the universe of "armed attacks" is narrower than that of a "use of force," also prohibited under international law. Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 844 (2012). Thus, it is possible for acts to violate prohibitions on the use of force but not trigger a right of self-defense under international law. *Id.* This means that a use of force in response to a cyberattack that arguably was a use of force but did not meet the test for an armed attack may violate a state's international legal obligations.

46. *See* NRC REPORT, *supra* note 6, at 33–34. The NRC Report is one of many analyses that have considered this issue to adopt such an approach. *See, e.g.*, CLARKE & KNAKE, *supra* note 8, at 178; Waxman, *supra* note 15, at 431–32; Matthew Hoisington, Comment, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. INT'L & COMP. L. REV. 439, 447–49 (2009).

47. *See, e.g.*, Lin, *supra* note 41, at 73; Hoisington, *supra* note 46, at 452.

48. This complexity is discussed in NRC REPORT, *supra* note 6, at 257–59, and Lin, *supra* note 41, at 80–82.

49. *See* NRC REPORT, *supra* note 6, at 257; Lin, *supra* note 41, at 80.

50. *See supra* note 49.

51. *See* Lin, *supra* note 41, at 74, 80–82. Dr. Lin argues that a sustained attack that shut down stock trading would almost certainly be considered a use of force, even absent physical destruction, but notes that there is an open question when it comes to mere manipulation of information and a resulting loss of public confidence. *Id.* at 74.

52. Lin makes this same distinction. *See id.* at 81–82.

If the issue is whether the military can carry out cyberattacks as a general matter, these line-drawing difficulties are far from merely academic; the United States might wish to carry out a cyberattack without triggering a right for the target to respond with traditional force under international law. Alternatively, the United States may choose to respond to a cyberattack with one of its own. If the initial attack is not an armed attack but the response *is* a use of force,[53] the American attack could create profound diplomatic and security troubles for the United States. Whichever legal regime is chosen, it should give a policymaker pause to think that a cyberattack, if undertaken by military authorities, could be done with significantly less congressional oversight than a covert action would require.[54] This in turn means less opportunity for persons outside the executive branch to weigh in on the wisdom of the proposed action.

The difficulties only increase when the question of whom to target arises. Not only are cyberattacks extremely difficult to trace definitively to their origins, but the wide availability of information technology and the ability to operate from virtually anywhere means that the target (or perpetrator) of a cyberattack could be a state or more problematically, a terrorist organization, criminal group, or an individual.[55] Obviously, these nonstate actors can all operate within the territory of a state. The attribution difficulty means that nonstate actors may be able to operate on a digital plane without detection by either the state in which they operate or a state (like the United States) that wishes to target them.

Two important consequences flow from the attribution difficulty in a scenario where the United States carries out a cyberattack in response to a cyberattack by a nonstate actor. First, the United States may be attacking the wrong people. Almost as importantly, even if the original attack can be definitively traced to its source, the state from which the group operated may have nothing to do with the conflict.[56] For example, suppose the United States sustained a cyberattack on its critical infrastructure and wished to

---

53. Such a scenario is more than plausible given that the indirect effects of cyberattacks are often more harmful than the direct effects, and more importantly, are extremely difficult for the cyberattacker to predict or control. *See* NRC REPORT, *supra* note 6, at 30–31, 80–81, 113–14. For the distinction between "armed attack" and "use of force," see *supra* note 45.

54. *See* Smith, *supra* note 11, at 546–47.

55. NRC REPORT, *supra* note 6, at 81, 138–41, 273–79; Goldsmith, *supra* note 8. Of course, one could easily argue that the difficulty of applying the law of war outside the context of the state system is endemic in modern conflict, but the features of cyberwarfare certainly exacerbate the issue.

56. This is little different from the case with kinetic warfare and the problems of terrorist groups operating within states that do not support them. Cyberattacks, however, have the (un)fortunate combination of seeming invisible in some ways, *see* Goldsmith, *supra* note 8 (arguing that the American public is largely ignorant of the threat of cyberattack and cyberexploitation because of their general isolation from computer networks and difficulty perceiving the threat), yet having the potential to cause effects every bit as devastating as kinetic strikes. This might have the troubling tendency of encouraging the use of cyberattacks in the mistaken belief that they are an easy alternative to traditional force. *See* NRC REPORT, *supra* note 6, at 50.

respond with its own cyberattack, only to discover that the attack originated from a small group of terrorists using computers in an allied country (and that the attack probably passed through computer networks in many allies' territories).[57] If a responsive cyberattack were to affect, for example, access to the internet in those allied countries,[58] the attack may be inappropriate or, in extreme circumstances, may be best done covertly, which would allow the United States to disavow its actions.[59]

C. *The Covert Action Regime: Some Advantages and a Limitation*

This Section explains that the covert action framework provides a source of authority for a broader range of cyberattacks than military authorities do, and addresses the advantages of the covert action framework over those of the military regime, as well as an important limitation on covert action. This Section first discusses the advantages of the covert action framework, such as a wider range of covered activities and the ability to avoid the boundary problems arising from the similarity between cyberattacks and cyberexploitations. This Section next argues that the covert action framework provides a single regime under which any appropriate U.S. agency or department could conduct cyberattacks under one set of legal rules. The covert action regime's considerable flexibility also tracks the emerging convergence of military and intelligence functions in twenty-first-century warfare. Finally, this Section addresses the important "traditional military activities" exception to the covert action requirements and the analytical challenge it poses in the case of cyberattacks.

The covert action framework offers advantages over those of the military framework when it comes to cyberattacks. At the most basic level, covert action captures a range of activities that the military framework does not. For example, suppose that the government thought it was necessary to alter data in a foreign bank that it believed was being used by a terrorist group. The military could not plausibly construe this action as preparation of any battlefield, and (depending on the bank's location) the bank would be unlikely to be the target of future armed conflict.[60] Indeed, even when there is potential for a future armed conflict, some activities not targeted directly at the state's apparatus may be initiated as covert actions even if the target could be legitimately struck by the military in wartime. For example, some have alleged that in 1982, the United States doctored software that controlled the pumps and valves of a Soviet natural gas pipeline, causing an

57. Some scholars have discussed the need for a doctrine of cyberneutrality, since many malicious activities in cyberspace travel through countries with no connection to the attackers. *See* NRC REPORT, *supra* note 6, at 268–69.

58. Or even something more serious, like a power grid.

59. *See* NRC REPORT, *supra* note 6, at 141 (noting that the difficulty of attribution means cyberattacks can often be carried out with a high level of deniability).

60. *See* WILLIAM J. DAUGHERTY, EXECUTIVE SECRETS 88 (2004).

explosion.[61] Aside from these more sensational possibilities, there are many gradations of alteration or disruption of computer programs or networks abroad. Very few of these would involve military purposes, but all would be cyberattacks, and their indirect effects would be difficult to predict.[62]

There are reasons beyond the statute's broader range of covered activities to prefer the covert action statute to military legal authority. One significant consideration is the technical similarity between cyberattacks and cyberexploitations. Because these two types of cyberoperations are distinguished primarily by the intent of the actor,[63] prudence might suggest that the covert action statute is a stronger basis on which to initiate cyberexploitations, which could evolve rapidly into cyberattacks. The unpredictable effects of operations over a computer network mean that what starts as espionage conducted by the intelligence apparatus can transform into an activity that changes the targeted program or network.[64] Therefore, the agencies that conduct cyberexploitations would benefit from the greater latitude to conduct cyberattacks that comes with the covert action regime, and use of the covert action regime would also cause agency personnel to err on the side of reporting their activities to the congressional committees.

The covert action statute is a flexible regime for operations that lie at the border separating military from intelligence activities. This is so because it provides a single framework that can be used by any agency,[65] and such broad use is well suited to the emerging reality of increased convergence of military and intelligence functions. The definition of covert action is "act-based, not actor-based."[66] Indeed, the covert action framework can be employed even

---

61. NRC REPORT, *supra* note 6, at 195. According to former national security official Thomas Reed, American intelligence learned of Soviet plans to steal Canadian software to automate operations at a trans-Siberian oil pipeline. U.S. intelligence modified the software in advance of its theft, and several months after installation, the stolen codes caused pump speeds and valves to induce more pressure than the pipeline could take, causing a massive explosion. THOMAS C. REED, AT THE ABYSS: AN INSIDER'S HISTORY OF THE COLD WAR 267–69 (2004). Importantly, this action, if true, took place before the statutory reporting requirement was implemented.

62. *See supra* note 53.

63. *See supra* note 10 and accompanying text.

64. *See* Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1199–2000 (2011).

65. Though covert actions are generally carried out by the Central Intelligence Agency ("CIA"), the statute's language applies to any agency tasked with carrying out the activity. *See* 50 U.S.C. § 413b(a)(3) (2006). There is an executive order stating that only the CIA (or the military in a time of war declared by Congress) will conduct "special activities," but also that the president may designate another agency to do so if it is appropriate to the mission. Exec. Order No. 12,333, § 1.8(e), 3 C.F.R. 200, 206 (1982), *reprinted as amended in* 50 U.S.C. § 401 note at 542, 545 (2006). In the case of cyberattack, the National Security Agency ("NSA") may often be the best fit. *See* CLARKE & KNAKE, *supra* note 8, at 37 (calling NSA "the world's premier electronic intelligence organization").

66. BAKER, *supra* note 24, at 151. Though Judge Baker admits that the numerous exceptions in the statute put pressure on this claim, *see id.* at 151–57, it is abundantly clear from the language of the statute itself, *see* 50 U.S.C. § 413b(e), and from the statute's sanctioning of covert actions by other agencies and departments, *see id.* § 413b(a)(3).

when military authority is equally available. For example, even though Osama bin Laden was clearly within the scope of a congressional authorization to use force,[67] U.S. policymakers decided to carry out a kill mission under the covert action framework.[68] Moreover, after the success of the mission, the United States clearly made no effort to conceal its own role. Had the operation failed though, the covert action framework would have offered deniability, as opposed to merely secrecy. Thus, an operation under military legal authority can also be conducted in secret under the covert action framework. Also, by ensuring prior notification to members of Congress, the covert action framework means members would know of a high-risk decision and could express a (nonbinding) view that might inform the decisionmaking.[69] In the case of the bin Laden mission, congressional notification was a politically astute move, regardless of whether the committee members actually expressed substantive thoughts on the operation; the notification gave President Obama a means to try to diffuse blame for a failed mission by noting knowledge (and perhaps tacit approval) of the plan on the part of members of Congress. It also allowed the Central Intelligence Agency ("CIA"), an agency with a great deal of covert action experience, to take the operational lead.[70]

The covert action framework is not a panacea for all of the difficulties of applying military authorities to cyberattacks, however. For one thing, a covert action that constitutes a use of force must comply with the law of armed conflict, regardless of whether U.S. military or civilian personnel carry it out.[71] Indeed, the covert action statute itself lays out some important limitations. Most broadly, no covert action can be conducted that "would violate the Constitution or laws of the United States."[72]

There is a view that a broad range of deniable cyberattacks may be carried out by the military under the covert action statute's exception for "traditional . . . military activities or routine support to such activities[,]"[73]

---

67. Robert Chesney, *What If Anything Does UBL's Death Mean for the AUMF?*, LAWFARE (May 2, 2011, 1:22 PM), http://www.lawfareblog.com/2011/05/what-if-anything-does-ubl%E2%80%99s-death-mean-for-the-aumf/.

68. Robert Chesney, *On the Legality of Killing UBL Even If He Was Unarmed (and On the Title 50 Issue)*, LAWFARE (May 4, 2011, 11:15 AM), http://www.lawfareblog.com/2011/05/on-the-legality-of-killing-ubl-even-if-he-was-unarmed-and-on-the-title-50-issue/ (stating that then-CIA Director Leon Panetta had specifically acknowledged that the raid to kill bin Laden was a title 50 operation). This highlights the possibility that even events that will later be trumpeted publicly (rather than denied) can be carried out under the statute with its presidential finding and congressional reporting requirements.

69. The importance of congressional involvement as a policy matter is discussed *infra* Part III.

70. *See* Nicholas Schmidle, *Getting bin Laden: Inside the Raid in Abbottabad*, NEW YORKER, Aug. 8, 2011, at 34, 38.

71. *See* W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION 77 (1992).

72. 50 U.S.C. § 413b(a)(5) (2006).

73. *Id.* § 413b(e)(2).

thus evading the finding and reporting requirements.[74] But taken to extremes, this perspective would render the covert action statute meaningless. Admittedly, the National Defense Authorization Act for Fiscal Year 2012 does recognize military authority to conduct cyberattacks[75] and the Act's legislative history reveals that Congress meant to affirm that some cyberattacks can be traditional military activities carried out under the same regime that governs kinetic capabilities.[76] Further, the covert action statute's own legislative history suggests that Congress meant to exclude from the reporting requirement activities that were carried out under a military commander or that constituted routine support for a military operation, even if carried out well in advance of anticipated hostilities.[77]

However, the argument taken too far recognizes almost no limits on the military's ability to conduct cyberattacks (or many other military operations) free of legislative oversight. In the case of an acknowledged conflict, even if the operation itself is secret, there is indeed a strong basis for claiming the exception. Presumably, in that scenario, either Congress has authorized the hostilities in general, or the president is exercising his constitutional power to defend the nation from attack.[78] But it is not plausible to suggest that routine support for anticipated hostilities (which would fall into the exception) includes penetration of foreign networks that begins years, if not decades, before hostilities.[79] That interpretation is undesirable because it could entirely prevent members of Congress from being informed of ongoing cyberattacks by the United States.[80] Cyberattacks' potential for massive indirect effects that cannot be reliably estimated ex ante makes this a more serious problem than many other secret military operations might pose. The perspective of even a few members of Congress might go far in increasing

---

74. *See, e.g.*, Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar"*, 22 FLA. J. INT'L L. 333, 335–45 (2010).

75. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) (codified as note to 10 U.S.C. § 111 (Supp. V 2011)).

76. *See* H.R. REP. No. 112-329, at 686 (2011) (Conf. Rep.), *reprinted in* 2011 U.S.C.C.A.N. 963, 1076.

77. *See* RICHARD A. BEST, JR., CONG. RESEARCH SERV., RL 33715, COVERT ACTION: LEGISLATIVE BACKGROUND AND POSSIBLE POLICY QUESTIONS 7–8 (2011); Walker, *supra* note 74, at 340–41.

78. For more on the importance of authorizations to use force, and their relationship to this Note's argument, see *supra* Part II. A military cyberattack meant to disrupt the planning of attacks on U.S. forces in Iraq, which could easily be framed as falling within the congressional authorization to use force in Iraq, Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 116 Stat. 1498 (codified as note to 50 U.S.C. § 1541 (2006)), apparently disrupted more than 300 servers in Saudi Arabia, Germany, and Texas, Ellen Nakashima, *Dismantling of Saudi-CIA Web Site Illustrates Need for Clearer Cyberwar Policies*, WASH. POST, Mar. 19, 2010, at A1. Those are the type of potential consequences that would have made congressional notification under title 50 desirable.

79. This type of long-term planning has precedent in kinetic warfare. *See* Walker, *supra* note 74, at 342–43.

80. *Id.* at 335. Reasonable persons can differ, however, on the wisdom of this interpretation as a matter of policy. *See id.* at 335 n.13.

the amount of consideration that would precede such operations.[81] More importantly, as a matter of statutory interpretation, reading the finding and reporting requirements into oblivion in cases of preparation far in advance of conflict seems to fly in the face of the animating purpose of a statute enacted in the wake of executive excess.[82]

The covert action statute enables the military, the CIA, the National Security Agency ("NSA"), and any other entity that may plausibly conduct cyberattacks targeted abroad to do so pursuant to the same legal framework of findings and reporting requirements. This unity of legal authority will be useful as the lines between intelligence and military functions continue to blur.[83] The covert action statute serves as a cautious choice when it is difficult to ascertain whether a cyberattack is a use of force or not, or a traditional military activity or not. If a particular cyberattack that was meant to be deniable is not considered a traditional military activity or within the scope of the military's mission, failing to comply with the title 50 requirements would be a statutory violation by the executive. Meeting the threat of terrorist organizations, individuals, or other targets (whether in the physical world or cyberspace) whose locations may prevent traditional kinetic strikes may call for more than can be delivered with cyberexploitations, and less than what the military could do in a recognized conflict.

II. THE COVERT ACTION STATUTE AS AN INDEPENDENT DOMESTIC LEGAL BASIS FOR USE OF FORCE

If a cyberattack rising to the level of a use of force is carried out against a target not covered by a congressional authorization to use force, the covert action statute would endow the president with greater constitutional legitimacy in ordering the attack than would independent presidential authority alone. To support this claim, Section II.A provides an overview of separation of powers doctrine generally and constitutional

---

81. *See* Jack Goldsmith, *Fire When Ready*, FOREIGN POL'Y, Mar. 19, 2012, http://www.foreignpolicy.com/articles/2012/03/19/fire_when_ready (noting that members of intelligence committees have many ways to push back against proposed covert actions they do not like).

82. *See supra* note 24 and accompanying text.

83. *See, e.g.*, Robert Chesney, *The al-Aulaqi Strike and Military-Intelligence Convergence*, LAWFARE (Oct. 2, 2011, 3:58 PM), http://www.lawfareblog.com/2011/10/the-al-aulaqi-strike-and-military-intelligence-convergence/ (noting in reference to drone strikes in Yemen the close cooperation of the military and CIA and the merging of their technical capacities, as well as the questions convergence raises for the respective legal regimes governing intelligence and the military); *see also* Josh Gerstein, *Sept. 11 Panel's Forgotten Concern: 'Paramilitary' CIA*, POLITICO (Sept. 10, 2011, 2:54 PM), http://www.politico.com/news/stories/0911/63155.html (noting that the Obama Administration has increased the scope of the CIA's paramilitary operations program). In another sign of this phenomenon, the director of the National Security Agency is "dual hatted" as the commander of the U.S. military's Cyber Command. CLARKE & KNAKE, *supra* note 8, at 39. Moreover, consider Secretary Panetta's move from the CIA to his present post at the Department of Defense, and General Petraeus's contemporaneous switch to head of the CIA. Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 579.

war powers in particular. Next, Section II.B argues that the covert action statute can plausibly be read to provide congressional support for certain uses of force, based on its text and the executive's history of interpreting statutes originally meant to limit executive authority as affirmations of presidential power. In addition, the textual limits in the covert action statute are consistent with those necessary for Congress to delegate to the president certain powers.

A. *Separation of Powers and Constitutional War Powers*

It has become axiomatic of American constitutional doctrine that presidential decisions gain greater constitutional legitimacy when they are carried out with Congress's approval. Though the president has tremendous freedom to act autonomously when conducting foreign affairs, the concerted action of both elected branches strengthens the presumption that the presidential policy is lawful. It is unclear, however, what the respective powers of either branch are when the president and Congress actively oppose one another, or when the president acts in the face of congressional silence.[84] In the exercise of constitutional war powers, it seems clear that the president can order the responsive use of force, but becomes less so when faced with the question of whether the president may initiate an armed conflict. Congress is probably empowered to place substantive limits on the scope of hostilities and the initiation of conflicts.

Perhaps the best-known statement of the approach for assessing the relative power of the executive comes from the Supreme Court's decision in *Youngstown Sheet & Tube Co. v. Sawyer*.[85] In a concurring opinion, Justice Jackson established a famous, if enigmatic, framework for resolving separation of powers questions. Jackson divided the world of presidential action into three categories. In the first (typically referred to as "Category I"), "the President acts pursuant to an express or implied authorization of Congress, [and] his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."[86] In this scenario, the president acts essentially with the total power of the federal government, and presidential decisions will be supported by the strongest presumptions of constitutional validity.[87] In the next category ("Category II"), Jackson states cryptically that when the president acts in the face of congressional silence, there exists a "zone of twilight," in which the president can only rely on his inherent constitutional powers for authority, and the powers of the president and Congress may be concurrent.[88] Finally, there is a third sphere ("Category III"), in which the president's actions contradict the will of Congress. In this third sphere, the president's power is at its "lowest ebb,"

84. *See infra* notes 86–91 and accompanying text.

85. 343 U.S. 579 (1952).

86. *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

87. *Id.* at 635–37.

88. *Id.* at 637.

and can only be proper if the president's constitutional authority under the circumstances outweighs that of Congress.[89] Such a collision requires careful scrutiny so as not to upset the balance of powers within constitutional system.[90] The Court has adopted Jackson's framework as controlling.[91]

Applying this general scheme to war powers is especially difficult because of the uncertainty surrounding the constitutional division of those powers.[92] The Constitution's text itself provides few clear answers. The president is notably made commander-in-chief of the military, without explanation of what that title means.[93] The president is also vested, again without clear definition, with "the executive Power."[94] However, Congress is also given grants of authority in war, including the power to declare war,[95] provide for the raising of armies and navies,[96] make rules to govern the military,[97] and "provide for the common [defense]."[98]

Scholars seeking to ascertain the Framers' original intent for those clauses and the provisions' original meanings have generally concluded that the president and Congress share warmaking powers, and that congressional authorization is needed to initiate a war. None of the Framers "wanted either to deny the [p]resident the power to respond to surprise attack or to give the [p]resident general power to initiate hostilities."[99] Several early Supreme Court cases interpreting the constitutional text seem to confirm this, and they assign Congress the primary role in deciding when to enter war.[100] As for the meaning of the Commander-in-Chief Clause, it is clear that it was not merely honorific, but rather implied some substantive authority as well.[101] At the very least, Congress may not delegate command of the armed forces to anyone other than the president, who will be the person to direct military activities as authorized by Congress.[102] While the

89. *Id.* at 637–38.

90. *Id.*

91. *See* Dames & Moore v. Regan, 453 U.S. 654, 668–69, 672–78 (1981) (discussing and applying Jackson's framework).

92. *See* Julian Davis Mortenson, *Executive Power and the Discipline of History*, 78 U. CHI. L. REV. 377, 377–78 (2011) (book review).

93. *See* U.S. CONST. art. II, § 2, cl. 1.

94. *Id.* § 1, cl. 1.

95. *Id.* art. I, § 8, cl. 11.

96. *Id.* cls. 12–13.

97. *Id.* cl. 14.

98. *Id.* cl. 1.

99. ARTHUR M. SCHLESINGER, JR., THE IMPERIAL PRESIDENCY 4 (1973).

100. *E.g.*, Talbot v. Seeman, 5 U.S. (1 Cranch) 1, 28 (1801) (stating that the Constitution vests the warmaking power in Congress and that Congress may authorize hostilities); *see also* Stephen I. Vladeck, *Congress, the Commander-in-Chief, and the Separation of Powers After* Hamdan, 16 TRANSNAT'L L. & CONTEMP. PROBS. 933, 935–36 (2007).

101. David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—Framing the Problem, Doctrine, and Original Understanding*, 121 HARV. L. REV. 689, 767 (2008).

102. *See id.* at 767–68; *see also* SCHLESINGER, JR., *supra* note 99, at 5–6.

Commander-in-Chief Clause does seem to imbue the president with some inviolable powers to direct the military, history suggests that the power to command was not an unlimited power to use the military when and as the president saw fit.[103]

On questions of executive power, practice and tradition are also important interpretive tools,[104] and the history of executive practice indicates that while presidents have often taken an expansive view of their substantive warmaking powers, Congress has also played a significant role in cabining presidents' authority to initiate certain conflicts and in defining actions that a president may take in war. "Deeply embedded traditional ways of conducting government cannot supplant the Constitution or legislation, but they give meaning to the words of a text or supply them."[105] When looking for the contours of the executive power with which the Constitution vests the president, it is relevant to look to long, unbroken traditions of presidential practices that have never been challenged by Congress.[106] In the case of warmaking, the relevant history shows that "[p]residents have long operated" under the assumption that their conduct in war was subject to some degree of congressional control, "and . . . have adjusted their actions" in response to such control.[107] Thus, the view that presidents' commander-in-chief power established a monopoly over the use of force preclusive of congressional control is mistaken.[108]

---

103. Barron & Lederman, *supra* note 101, at 800. There is a minority view that the Commander-in-Chief Clause granted a preclusive substantive power to authorize hostilities to the president, and that Congress's power to declare war meant nothing other than the power to recognize the legal status of war. *See, e.g.*, JOHN YOO, THE POWERS OF WAR AND PEACE 144–52 (2005). However, Professor Yoo's position has been sharply criticized. *See, e.g.*, Mortenson, *supra* note 92, at 393–97. Professor Mortenson argues that "Yoo's discussion of the Founding is thoroughly unconvincing on any of the national security questions that matter." *Id.* at 397.

104. *See* SCHLESINGER, JR., *supra* note 99, at 13 ("[W]hat the Constitution 'really' meant . . . in practice . . . only [actual] practice could disclose."); *see also* Curtis A. Bradley & Trevor W. Morrison, *Historical Gloss and the Separation of Powers*, 126 HARV. L. REV. (forthcoming 2012) (manuscript at 6–7), *available at* http://ssrn.com/abstract=1999516.

105. Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 610 (1952) (Frankfurter, J., concurring).

106. *Id.* at 610–11; *see also* HAROLD HONGJU KOH, THE NATIONAL SECURITY CONSTITUTION 70–71 (1990) (describing the importance of precedential actions in determining "quasi-constitutional custom" in national security affairs). Importantly, while Justice Frankfurter's opinion is often seen as a gloss on situations in which the president acts and Congress is silent, and Barron & Lederman, *infra* note 107, discuss the history of the clash of presidential and congressional will, both emphasize the importance of history and tradition in addressing questions of the relative powers of the elected branches.

107. David J. Barron & Martin S. Lederman, *The Commander in Chief at the Lowest Ebb—A Constitutional History*, 121 HARV. L. REV. 941, 1101 (2008).

108. *Id.* at 1100. Again, Yoo has a different perspective. *See* Yoo, *supra* note 103, at 155–60 (arguing that recent history comports with a view of nearly unfettered executive power in war, and that Congress's only recourses involve defunding operations or impeachment). But, for a rebuttal of other claims along similar lines, see Mortenson, *supra* note 92, at 425–30.

Constitutional text and history, executive practice, and scholarly commentary seem to establish that some role for Congress is necessary when the president initiates hostilities.[109] Even the Office of Legal Counsel, which because of its institutional position can be expected to assert a broad view of executive power,[110] has recognized Congress's authority to put a sixty-day limit on presidential deployment of troops into hostilities, to require consultation when the president does order entry into hostilities, and even to order the withdrawal of troops via legislation.[111] As for those deployments that are authorized, Congress need not directly issue a declaration of war using those precise words. Rather, it seems that Congress has more flexibility to choose the language authorizing force.[112] The next Section questions whether the covert action statute might qualify as such an authorization in certain circumstances.

B. *Cyberattacks, Force, and Covert Action*

This Section applies the separation of powers and war powers analysis to cyberattacks. Section II.B.1 argues that initiating cyberattacks that are not a use of force under the covert action statute can elevate the operation to *Youngstown* Category I, where it would enjoy the greatest presumption of constitutional legitimacy. If a cyberattack would be a use of force—or more likely, if it is unclear whether it would approximate a use of force—and the attack would not be in support of an ongoing conflict already authorized by Congress, then the cyberattack would trigger the war powers requirements, and congressional approval would be needed.[113] Section II.B.2 contends that the covert action statute might conceivably meet the requirement for congressional authorization for those cyberattacks that do necessitate a war powers analysis. This is because of the statute's text, the executive practice of interpreting statutes as affirmations of executive power, and the claim's consistency with limits on congressional delegations of power to the president.

---

109. *See supra* notes 92–108 and accompanying text.

110. *See* JACK GOLDSMITH, THE TERROR PRESIDENCY 34–35 (2009).

111. Presidential Power to Use Armed Forces Abroad Without Statutory Authorization, 4A Op. O.L.C. 185, 186, 195–96 (1980). *But see* Deployment of U.S. Armed Forces to Haiti, 28 Op. O.L.C., 2004 WL 5743904, at *5 (Mar. 17, 2004) (declining to decide the constitutionality of the War Powers Resolution).

112. Doe v. Bush, 323 F.3d 133, 144 (1st Cir. 2003) (noting that the Iraq War Resolution is by its terms an authorization for the president to use military force); *see also* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2057–62 (2005).

113. Even if the "congressionalist" view of war powers articulated in *supra* Section II.A is incorrect, presidential decisions to go to war in the absence of congressional support would still be in *Youngstown* Category II, and those decisions would have a firmer constitutional foothold if made pursuant to some congressional authorization, which might include, as I argue, the covert action statute.

1. Cyberattacks, *Youngstown*, and War Powers

Depending on the type of cyberattack and the legal framework applied, the action might fall into any of Justice Jackson's *Youngstown* categories, but in many circumstances, compliance with the covert action statute will elevate the operation into Category I. Given the broad statutory definition of covert action,[114] it seems that any cyberattack that does not fall into one of the covert action statute's exceptions[115] and is meant to be deniable would trigger the statute's finding and reporting requirements. The statute states that the president "may not authorize the conduct of a covert action" without meeting the necessary requirements.[116] A president who ordered an attack without following the finding and reporting procedures would therefore be in Category III, where presidential authority is at its lowest. Conversely, complying with the covert action statute's requirements would place the operation in a higher *Youngstown* category than would using the military framework.

As for those cyberattacks that *do* generate sufficient effects outside cyberspace to constitute a use of force and thus require a war powers analysis—under which the president can rely on inherent executive power for responsive force but must have congressional support to initiate offensive conflict—surely some could be exempt from the definition of covert action under the traditional military activities exception,[117] but that does not resolve the separation of powers issue. If a cyberattack that approximated a use of force were ordered without a statutory authorization to use force against that entity, the operation would exceed the president's war powers.[118] Relying on the covert action procedures, especially when it is unclear whether a specific cyberattack would qualify as a traditional military activity, could ensure a stronger presumption of constitutional validity. No special congressional authorization seems necessary for those cyberattacks—even the ones that constitute a use of force—that are initiated in support of an ongoing conflict already authorized by Congress. But outside this scenario, cyberattacks that constitute a use of force require congressional approval under the Constitution's division of war powers.

The National Defense Authorization Act for Fiscal Year 2012 speaks specifically to cyberattacks, but it cannot be read convincingly as a general authorization to conduct cyberattacks that would constitute force. The Act states that "Congress affirms that the Department of Defense has the capability, and . . . may conduct offensive operations in cyberspace" subject to

---

114. *See* 50 U.S.C. § 413b(e) (2006).

115. *See id.* § 413b(e)(1)–(5).

116. *Id.* § 413b(a).

117. *See id.* § 413b(e)(2); *see also supra* notes 26, 73–77 and accompanying text. However, the arguments discussed at *supra* notes 78–82 and accompanying text suggest that this may not always be the case, and that the covert action framework still exists as an available option.

118. Again, even rejecting the view that Congress must assent to the initiation of use of force, at best such an operation would be in *Youngstown* Category II.

the "policy principles and legal regimes that the Department follows for kinetic capabilities" and the War Powers Resolution.[119] On one reading, this provision is a blanket authorization for cyberattacks. But that would ignore both the full text of the statute and its legislative history. The statute specifically notes that the authority is subject to the legal regimes that govern kinetic operations.[120] This language seems to disclaim any pretense of altering the substantive legal regime that would apply to the operation. Moreover, the legislative history makes clear that the purpose of the bill was to confirm that notwithstanding their novelty, cyberattacks can indeed qualify as traditional military activities.[121] The section of the statute dealing with cyberattacks is likely premised on the assumption of some preexisting authorization to use force, as opposed to a new grant of authority.[122] A better reading, then, is that the statute merely resolves any confusion over whether the military can conduct cyberattacks at all. This Note assumes it can, but one must look elsewhere for a plausible candidate for congressional authorization to conduct cyberattacks that amount to a use of force.

2. The Covert Action Statute as Authorization to Use Force

The requirement for congressional authorization under a war powers analysis would be met if the covert action statute itself could sometimes function as a limited authorization to use force. This question has not been extensively explored in the academic literature. The suggestion that the covert action statute might provide such an independent domestic legal basis to use force appears to have been suggested first by Martin Lederman, professor of law at Georgetown University Law Center, writing on a legal blog.[123] Discussing the possible domestic legal bases for the operation that killed Osama bin Laden, Lederman briefly mentioned covert action. While bin Laden was indeed covered by an existing authorization to use military force, the covert action statute "might have been a second source of domestic

---

119. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) (codified as note to 10 U.S.C. § 111 (Supp. V 2011)).

120. *Id.*

121. H.R. REP. No. 112-329, at 686 (2011) (Conf. Rep.), *reprinted in* 2011 U.S.C.C.A.N. 963, 1076. This view is consistent with a provision in an earlier version of the legislation that authorizes the military to conduct cyberattacks pursuant to the Authorization for the Use of Military Force of September 2001, or in response to an attack on an asset of the Department of the Defense, rather than a general authorization to use force so long as it is in cyberspace. *See* H.R. 1540, 112th Cong. § 962 (as passed by House, May 26, 2011). It is similarly consistent with language that would amend the provision in the pending National Defense Authorization Act for Fiscal Year 2013. *See* H.R. 4310, 112th Cong. § 941 (as passed by House, May 18, 2012).

122. *See* Chesney, *Offensive Cyberspace Operations*, *supra* note 38.

123. Marty Lederman, *The U.S. Perspective on the Legal Basis for the bin Laden Operation*, BALKINIZATION (May 24, 2011, 12:31 AM), http://balkin.blogspot.com/2011/05/us-perspective-on-legal-basis-for-bin.html.

authority."[124] That is the full extent of the suggestion. On another blog, Robert Chesney, professor of law at the University of Texas School of Law, responded, saying that surely some activities that might be undertaken pursuant to the covert action statute are "of sufficient intensity that they would demand a war powers analysis if conducted openly."[125] Chesney wondered whether that analysis can be avoided entirely by making the decision to proceed under the covert action framework as an initial matter.[126]

Based on the text of the statute, it seems that a decision to proceed under the finding and reporting requirements places a cyberattack that constitutes a use of force on considerably firmer constitutional ground than one that relies solely on the president's inherent authority. The language of the statutory text itself should be given considerable weight in interpretation.[127] In this case, the statute defines covert actions as "activities" of the U.S. government meant "to influence political, economic, or military conditions abroad" where the hand of the United States "will not be apparent or acknowledged."[128] That language is very broad, and that breadth should inform the analysis. Force is not mentioned, but neither is it precluded. As long as the president complies with the conditions in the statute, it is reasonable to understand the statute as conferring congressional approval on covert actions.

A serious objection to this contention is that by excluding traditional military activities from the definition of covert action, the covert action statute *does* preclude its application to the use of force. However, this Section's argument is based on the contention that the universe of traditional military activities does not exhaust the universe of operations that involve sufficient force to trigger a war powers analysis. The difficulty is in discerning an analytically sound line to distinguish the two spheres. Some observers have argued that the technological novelty of cyberattacks cannot bar them from being traditional military activities, for the simple reason that the U.S. military has always been on the cutting edge of technology.[129] This view is certainly correct insofar as cyberattacks *can* be traditional military activities, but it does not follow that technological novelty does no analytical work

---

124. *Id.* At least in its public statements, the CIA—the agency most associated with covert action—does not appear to claim the covert action statute as an authorization to use force. *See* Stephen W. Preston, *CIA and the Rule of Law*, 6 J. NAT'L SECURITY L. & POL'Y 1, 6 (2012) (noting that use of force requires either inherent executive authority or specific congressional authorization).

125. Robert Chesney, *Title 50 as a Sufficient Domestic Law Predicate for Certain Uses of Force*, LAWFARE (May 24, 2011, 12:09 PM), http://www.lawfareblog.com/2011/05/title-50-as-a-sufficient-domestic-law-predicate-for-certain-uses-of-force/.

126. *Id.*

127. *See* Frank H. Easterbrook, *Text, History, and Structure in Statutory Interpretation*, 17 HARV. J.L. & PUB. POL'Y 61, 63–65 (1994) (highlighting the importance of giving primary weight to statutory text and the purposes that method serves).

128. 50 U.S.C. § 413b(e) (2006).

129. *See, e.g.*, Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SECURITY J. 591, 605 (2011), *available at* http://harvardnsj.org/wp-content/uploads/2011/02/Vol.-2_Bradbury_Final1.pdf.

under any circumstances. It seems that combining the characteristic features of cyberattacks—difficulty of attribution, remote access, and unpredictable effects—with a view of the traditional military activities exception that would include all uses of force would categorically exempt those cyberattacks that entail force from even the legislative oversight offered by the War Powers Resolution.[130] Specifically, though recent statutory enactments confirm that cyberattacks undertaken by the military must comply with the War Powers Resolution,[131] the Obama Administration's narrow reading of the resolution's reference to "hostilities"[132] makes it difficult to conceive of a cyberattack that would trigger the resolution's reporting requirements.[133] The fact that a particular view of the exception might allow a result *so* at odds with the resolution's purpose undercuts its theoretical soundness.

Concern for statutory purpose leads to another plausible objection to this position: the covert action statute was meant to restrain executive power rather than enhance it. The covert action statute was enacted after the Iran–Contra affair as a means of providing oversight to check the president's discretion in ordering covert activities to meet foreign policy objectives.[134] That background should arguably guard against an effort to transform the statute into a grant of authority.[135]

But that objection ignores a long history of executive responses to statutes that seek to define presidential power. The executive branch has a long-standing tradition of construing statutory definitions and limitations on presidential power as affirmations of authority.[136] Perverse though that logic may seem, it maps well onto the widely acknowledged constitutional significance that executive practice has when analyzing separation of powers questions.[137] One salient example is the War Powers Resolution, whose limitations have already been read so as not to apply to a wide range of activities.[138] The executive branch has interpreted the resolution, passed in the flurry of efforts to control executive power after Watergate and Vietnam, as a confirmation of the president's power to use the military in hostilities without specific statutory authorization.[139] Reading the limits imposed by the covert action statute as an affirmation, if not a grant of power, provided that the proper procedures are followed, would not be a dissimilar exercise. Moreover, because the broad language used to define covert action seems to

130. 50 U.S.C. §§ 1541–1448.

131. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) (codified as note to 10 U.S.C. § 111 (Supp. V 2011)).

132. *See supra* note 38 and accompanying text.

133. *See* Chesney, *Offensive Cyberspace Operations*, *supra* note 38.

134. *See supra* note 24 and accompanying text.

135. *But see* Easterbrook, *supra* note 127.

136. *See* KOH, *supra* note 106, at 117.

137. *See supra* notes 104–106 and accompanying text.

138. *See supra* note 38 and accompanying text.

139. *See, e.g.*, Proposed Deployment of U.S. Armed Forces into Bosnia, 19 Op. O.L.C. 327, 334–35 (1995).

invite such a construction, it is not nearly as objectionable as a strained interpretation of the War Powers Resolution that twists the term "hostilities" almost beyond recognition.

Whether the covert action statute can serve as a congressional authorization for the president to use at least some force is partly dependent on whether it is appropriate for Congress to delegate such authority in such a broadly worded statute. Congress may delegate its authority to another actor so long as the delegation includes some "intelligible principle" to which the actor must conform.[140] So long as "Congress clearly delineates the general policy, the public agency which is to apply it, and the boundaries of th[e] delegated authority," the delegation is constitutionally valid.[141] In the case of the covert action statute, Congress has placed the authority in the president, prescribed special procedures that must be followed, and specified that the president may not order the actions unless in support of a clear foreign policy objective. This satisfies the delegation test. Moreover, the delegation doctrine may have even less applicability in the case of war powers, where the powers of Congress and the president overlap; there is not merely a delegation but also an affirmation of existing authority.[142] Thus, there is more force to the suggestion that the covert action statute may provide a domestic legal basis for cyberattacks—even those that amount to a use of force—that includes both presidential and statutory support.

Though separation of powers analysis is normally applied as a tool for judicial scrutiny, whether a major cyberattack can be said to have been conducted with the blessing of both Congress and the president is of serious constitutional import. The fact that activities may not be subject to judicial review[143] makes it even more important that the two other major constitutional actors in the American system conduct themselves with their constitutional obligations in mind. Also, a careful understanding of how the separation of powers applies to a novel means of statecraft and warfare can contribute to the public understanding of the national constitutional ethos.[144] A cyberattack's massive potential for unintended consequences demands a cautious constitutional approach to the conduct. The covert action statute

---

140. Mistretta v. United States, 488 U.S. 361, 372 (1989) (quoting J.W. Hampton, Jr., & Co. v. United States, 276 U.S. 394, 409 (1928)) (internal quotation marks omitted).

141. *Id.* at 372–73 (quoting Am. Power & Light Co. v. SEC, 329 U.S. 90, 105 (1946)) (internal quotation marks omitted). Indeed, in the field of foreign affairs, there may be no limit on the powers Congress can delegate to the president. *See* United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 315–22 (1936).

142. *See* Doe v. Bush, 323 F.3d 133, 143 (1st Cir. 2003) (noting the lesser applicability of the delegation doctrine to foreign policy questions).

143. A suit alleging noncompliance with the covert action statute would most likely be dismissed for nonjusticiability. As of a September 19, 2012 Westlaw search, only two cases have even cited the covert action statute, and neither decided whether an action complied with the statutory requirements. *See In re* Nat'l Sec. Agency Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1122 (N.D. Cal. 2008); ACLU v. Dep't of Defense, 396 F. Supp. 2d 459, 462 (S.D.N.Y. 2005).

144. *Cf.* Barron & Lederman, *supra* note 107, at 1101 (describing a similar benefit of understanding the history of legislative constraint of executive power).

serves this function by enabling the president to act with congressional approval.

III. ENACTING THE COVERT ACTION REGIME AS PRESUMPTIVE VIA EXECUTIVE ORDER

Cyberattacks present a challenge for U.S. policymakers: they are difficult to locate within a clear legal category and there is a significant risk of uncontrollable consequences associated with their use. As a result, policymakers must choose a paradigm to govern their use that will ensure that the executive branch is held accountable and shares information with legislators.

This Part argues that the federal government should adopt the presumption that cyberattacks will be carried out under the covert action statute, and that the best way forward is for the president to issue an executive order making the covert action regime the presumptive framework for cyberattacks. It includes a brief discussion of why a president might willingly constrain her discretion by issuing the proposed executive order. It also shows that while the internal executive processes associated with both military and intelligence legal frameworks help mitigate the risk of cyberattacks' misuse by the executive, only the covert action regime provides an adequate role for Congress. Finally, this Part argues that the executive order option is preferable to one alternative proposed by scholars—enacting legislation—because of the practical difficulties of passing new legislation.

The covert action regime is the best approach for committing cyberattacks under the current law, as it would facilitate cooperation among executive agencies. The debate over which agency and set of legal authorities govern cyberattacks has caused no small amount of confusion.[145] Apparently, an Office of Legal Counsel ("OLC") memorandum declined to decide which legal regime should govern the use of cyberattacks, and the uncertainty has led to interagency squabbles, as well as confusion over how cyberattacks are to be regulated.[146] Establishing a presumptive answer would go far toward resolving this dispute.

Most importantly, adopting the covert action framework as the presumptive legal regime would be a principled way to help ensure constitutional legitimacy when the president orders a cyberattack.[147] There is also reason to believe that presidential power is intimately bound up in credibility, which in turn is largely dependent on the perception of presidential compliance with applicable domestic law.[148] A practice of complying with the covert action

145. *See* Ellen Nakashima, *Pentagon Is Debating Cyber-Attacks*, WASH. POST, Nov. 6, 2010, at A01.

146. *See id.*

147. *See generally supra* Section II.B.

148. *See* Richard H. Pildes, *Law and the President*, 125 HARV. L. REV. 1381, 1424 (2012) (book review).

regime for cyberattacks, both when they do not constitute a use of force and when it is unclear whether they do, is most likely to be in compliance with the law. Compliance with the covert action regime would also encourage covert action procedures in close cases without unduly restricting the executive's choice to use military authorities in appropriate circumstances.

The executive might also issue the proposed order, even though it would limit her freedom in some ways, because of the possible benefits of constraining future administrations or preempting legislative intervention.[149] For example, in this context, an administration may choose to follow the finding and reporting requirements in order to convince Congress that legislative intervention is unnecessary for proper oversight. This is acceptable if the covert action regime is in fact adequate on its own. Moreover, if greater statutory control over cyberattacks *is* needed, the information shared with Congress may give Congress the tools and knowledge of the issue necessary to craft related legislation.[150] Additionally, while executive orders are hardly binding, the inertia following adoption of an order may help constrain future administrations, which may be more or less trustworthy than the current one. Creating a presumption through an executive order also establishes a stable legal framework for cyberattacks that allows law to follow policy in this new field, and permits decisionmakers to learn more about the nature of cyberoperations before passing detailed statutes that may result in unintended consequences.

A presumption in favor of the title 50 regime for cyberattacks is also desirable because it comports with the reality of an executive constrained by its own internal processes. Though energy, dispatch, and secrecy are among the key advantages the executive possesses over Congress,[151] the existence of a professional bureaucratic corps, including many lawyers, within the executive branch can foster necessary deliberation about important policy decisions.[152] For issues on which there is disagreement among executive agencies, such as a potential turf war between the military and intelligence communities over control of cyberattacks, advisory and adjudicatory bodies such as the Office of Legal Counsel can play a constructive role.[153] Even on an issue such as the best legal regime to govern cyberattacks, which is es-

149. *See* Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801, 895–96 (2011).

150. *See* Heidi Kitrosser, *Congressional Oversight of National Security Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1090 (2008).

151. *See* THE FEDERALIST NO. 70 (Alexander Hamilton).

152. *See* Neal Kumar Katyal, Essay, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 YALE L.J. 2314, 2317 (2006).

153. *See* Trevor Morrison, *Constitutional Alarmism*, 124 HARV. L. REV. 1688, 1713–23 (2011) (reviewing BRUCE ACKERMAN, THE DECLINE AND FALL OF THE AMERICAN REPUBLIC (2010)) (defending the institutional value of OLC). Bruce Ackerman, whose book Professor Morrison was reviewing, responded with a less optimistic view of the OLC's value as a tool to cabin executive discretion. *See* Bruce Ackerman, *Lost Inside the Beltway: A Reply to Professor Morrison*, 124 HARV. L. REV. FORUM 13, 15–22 (2011), http://www.harvardlawreview.org/media/pdf/vol124forum_ackerman.pdf.

sentially a policy choice, the friction between different competing agencies itself can serve a checking function.[154]

Moreover, the covert action statute helps with the vital work of balancing the president's need for independence against the costs of an uninformed Congress,[155] especially on national security issues with such potential for unforeseeable diplomatic and military risks. The national interests at stake in the cyberattack context are too great to be left to the president alone.[156]

Some scholars have proposed a contrary view. On this view, the speed with which cyberspace events can play out makes it important for the legislative role to be clearly established via statutory reform in advance of any cyberattack by the United States.[157] Thus, proposals for extensive legislative intervention would help ensure Congress's appropriate role in deciding whether or not to go to war.[158] The notion of congressional participation is well in line with the view of shared constitutional war powers articulated earlier in this Note.[159] Moreover, congressional participation comports with an ideal of government decisionmaking where the branch most immediately accountable to voters has been given a chance to express its view. Discussing the covert action regime, Stephen Dycus, professor of law at Vermont Law School, expresses concern that only the smaller group of intelligence committee leaders and the leaders of each House will be informed, and that in general the reporting requirements do not ensure that Congress will obtain the information it needs to play a meaningful role in the discussion.[160] Additionally, there are concerns regarding the traditional military activities exception to the reporting requirements in the covert action statute.[161] Specifically, the worry is that the military might classify clandestine cyberwarfare activities as "operational preparation of the environment" and thereby skirt the reporting requirements, being accountable instead to the congressional armed services committees—which could create confusion.[162] Dycus's proposed legislative reforms include designating particular congressional committees to receive reports, forming a lead federal agency for cybersecurity, banning automated offensive responsive to a cyberattack, and crafting procedures to aid private networks that come under attack.[163]

However, this position is flawed because it dismisses the covert action statute as wholly inadequate to protecting the value of congressional participation, and gives short shrift to the non-warlike dimensions of many

---

154. *See* Katyal, *supra* note 152.

155. Kitrosser, *supra* note 150, at 1089.

156. *See, e.g.*, Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SECURITY L. & POL'Y 155, 158 (2010).

157. *Id.*

158. *Id.* at 171.

159. *See supra* Part II.

160. Dycus, *supra* note 156, at 159–60.

161. *See supra* Section I.C.

162. Dycus, *supra* note 156, at 161.

163. *Id.* at 167–71.

cyberattacks. The worry that motivates some of the proposals seems to ignore the many examples of cyberattacks—such as manipulation of electronic ballots in a foreign election or disseminating false information through foreign networks to affect media reports—that, outside normal contexts, could not plausibly fall under the military activities exception. Moreover, they underestimate the potential power of a presumption by the executive in favor of the covert action regime.

An executive order establishing such a presumptive posture of reporting could go a long way toward bringing Congress into the process. First, an order establishing written findings and congressional reporting as the default rule could cause momentum to settle around title 50 procedures for initiating cyberattacks.[164] Also, one scholar has argued that the most effective way to ensure congressional notification might not be changing the actual rules of who is to be notified and when, but rather implementing changes that encourage the executive branch to comply with existing requirements.[165]

Significantly more modest statutory interventions have also been proposed; however, statutory clarification may not be necessary to achieve their aims. Like Dycus, Robert Chesney is concerned about drawing lines between covert action and traditional military activity in the cyberattack context. He argues that it may be useful for Congress to clarify that the military may conduct those operations outside the title 50 framework when defending Pentagon assets or acting pursuant to a separate statute authorizing force.[166] Moreover, he suggests notifying the congressional armed services committees when such operations are likely to have effects that spill over into areas outside a zone of conflict.[167] But there need not be a legislative mandate for an executive practice of reporting cyberattacks to both intelligence and armed services committees. Moreover, as Chesney himself argues, under a proper understanding of the definitions in the covert action statute, where routine support for ongoing hostilities is exempt under the military activities exception, any cyberattack initiated in support of a conflict authorized by congressional statute would be exempt.[168] This view accords well with that articulated in this Note,[169] and an executive order setting covert action procedures as the default would hardly preclude forgoing that framework in appropriate circumstances; a presumption, after all, merely encourages findings and reporting when there is doubt about the appropriate framework.

---

164. RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE 8 (rev. & expanded ed. 2009) (using behavioral law and economics to support the claim that the choice of a default rule has a significant impact on outcomes); *see also* GRAHAM ALLISON & PHILIP ZELIKOW, ESSENCE OF DECISION 151–52 (2d ed. 1999) (noting the role of bureaucratic politics in effecting outcomes).

165. Kitrosser, *supra* note 150, at 1084.

166. Chesney, *Military-Intelligence Convergence*, *supra* note 11, at 544.

167. *Id.*

168. *Id.* at 628.

169. *See supra* Part II (arguing that the legitimacy of executive decisions to use force is enhanced by statutory support).

Finally, while urging Congress to clarify the law governing cyberattacks may be advisable, one should consider the reality that such legislation is very difficult to pass. Congress is notoriously slow to act and legislation is difficult to push through the arduous process to enactment. There are numerous stages in the process at which a bill, even on an issue of significant importance, can be stalled or killed.[170] For example, a bill may not be considered by its corresponding committee in either House, may be bogged down with amendments that cause it to lose support, or be subject to the Senate filibuster, among other "vetogates."[171] In the case of clarifying the appropriate procedures for conducting a cyberattack, there may be concern that such legislation, either by imposing substantive constraints or reporting requirements, will improperly burden the president on a national security issue of increasing importance. Congress as an institution tends to acquiesce to presidential prerogative in national security matters.[172] Further, given that Congress has recently addressed cyberattacks in legislation, albeit in an unhelpfully vague provision,[173] the possibility of expansive legislative clarification in the near future seems even more remote.

An executive order making the covert action regime presumptive for cyberattacks gives the executive branch considerable flexibility while also ensuring notification to Congress. A presumptive regime helps remove current confusion within the executive branch, as well as allows cyberattack policy to develop with members of Congress gaining access to information that may be helpful in crafting later statutory controls on the use of cyberattacks. Moreover, some proposals for immediate legislative intervention overestimate congressional will to legislate in this field and underestimate the protections for interbranch collaboration offered by the covert action regime.

CONCLUSION

The covert action framework is a flexible one that can be applied by any appropriate agency, whether intelligence or military. The legal regimes governing military action, by contrast, lack this flexibility. Moreover, the wide array of cyberattacks that are not of a warlike nature, along with potential confusion between cyberattacks and cyberexploitations, counsels in favor of the covert action framework. In limited circumstances, the covert action

---

170. William N. Eskridge, Jr., *Vetogates,* Chevron, *Preemption*, 83 NOTRE DAME L. REV. 1441, 1444 (2008).

171. *Id.* at 1444–47. Despite Congress's factfinding resources and the necessity of its intervention in certain areas, legislative paralysis can often result in a gap in lawmaking initiative that other bodies cannot fill. *See* Henry J. Friendly, *The Gap in Lawmaking—Judges Who Can't and Legislators Who Won't*, 63 COLUM. L. REV. 787, 792–94 (1963) (lamenting Congress's failure to provide adequate guidance even in areas of the law that have become creatures of statute). All legal writing should cite Judge Friendly somewhere.

172. KOH, *supra* note 106, at 123–33.

173. *See* National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 954, 125 Stat. 1298, 1551 (2011) (codified as note to 10 U.S.C. § 111 (Supp. V 2011)).

statute might serve as an alternative legal basis for certain uses of force, and adherence to the covert action procedures could move cyberattacks into a sphere of presidential authority entitled to a strong presumption of validity. Finally, an executive order making the covert action framework presumptive for cyberattacks is a more attainable goal than detailed legislation. Indeed, the reporting requirements of the covert action regime may both preserve accountability to Congress and enable legislative reform.