CYBER "HOSTILITIES" AND THE WAR POWERS RESOLUTION

ALLISON ARNOLD*

I. Introduction

The Pentagon appears to be advancing toward a more offensive strategy in cyberspace.[1] At the very least, there seems to be a growing acknowledgment of the U.S. military's offensive cyber capabilities. For example, the head of U.S. Cyber Command, General Keith Alexander, announced in March that the Pentagon will have thirteen offensive cyber teams by fall 2015.[2] In April, the U.S. Air Force classified six of its cyber capabilities as "weapons."[3] These recent pronouncements seem to increase the likelihood that the United States may engage in future offensive military activities in cyberspace.

It has become clear in the modern age that the cyber domain is as relevant for military activities as the domains of land, sea, air, and space.[4] The increased use of cyber operations in modern warfare has been well documented by scholars.[5] Much of the legal analysis on the use of cyber operations has focused on international law and the use of force.[6] This article turns from that debate to focus on U.S. domestic law

---

* Research Associate, Defense Policy and Arms Control, Congressional Research Service, Foreign Affairs, Defense, and Trade Division, Washington, D.C. J.D., 2013; B.A., 2001, Brigham Young University. Member of the Virginia State Bar. The author would like to thank Professor Eric Talbot Jensen for his mentoring and encouragement.

1 Tom Gjelten, *First Strike: US Cyber Warriors Seize the Offensive*, WORLD AFF. J., Jan./Feb. 2013, *available at* http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

2 Ellen Nakashima, *Pentagon Creates Teams to Launch Cyberattacks as Threat Grows*, WASH. POST, Mar. 12, 2013, *available at* http://articles.washingtonpost.com/2013-03-12/world/37645469_1_new-teams-national-security-threat-attacks.

3 Andrea Shalal-Esa, *Six U.S. Air Force Cyber Capabilities Designated "Weapons,"* REUTERS, Apr. 8, 2013, http://www.reuters.com/article/2013/04/09/net-us-cyber-airforce-weapons-idUSBRE93801B20130409 (designating the cyber capabilities as weapons to help the programs compete for funding and garner more attention and recognition).

4 *See* U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010).

5 *See* Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 775–76 (2012); Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, 304 (2010).

6 *See generally* Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STAN. J. INT'L L.

and the implications of congressional efforts to reach offensive operations in cyberspace.

At the end of 2011, Congress addressed "Military Activities in Cyberspace" in the National Defense Authorization Act for Fiscal Year 2012 (NDAA 2012).[7] As will be discussed in Part II, Congress made an effort to impact the governance of offensive military cyber operations by referring to a piece of domestic legislation known as the War Powers Resolution. The War Powers Resolution was enacted forty years ago over the veto of President Nixon.[8] There is a great deal of literature and scholarly debate about its constitutionality and adequacy.[9] This article will not attempt to revisit those issues, but will instead examine the limitations of Congress's reference to the War Powers Resolution and offensive military cyber operations in the NDAA 2012. This article proffers an in-depth analysis of the interaction between offensive military cyber operations and the "hostilities" triggering language of the War Powers Resolution. The article argues that under current practice, the executive branch is unlikely to deem stand-alone offensive military activities in cyberspace as "hostilities" that trigger the statute.

This article begins with an analysis of the "Military Activities in Cyberspace" section of the NDAA 2012 and its connection to the War Powers Resolution. Part III examines the record of the 1973 Congress to review how the term "hostilities" came to be the operative language of the War Powers Resolution. Part IV explores how the executive branch has explained which type of military activities it considers to be

---

207 (2002); Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. NAT'L SEC. L. & POL'Y 63 (2010); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999); 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 (2011).

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

[8] *See* Veto of the War Powers Resolution, 5 PUB. PAPERS 893 (Oct. 24, 1973).

[9] *See, e.g.*, Geoffrey S. Corn, *Triggering Congressional War Powers Notification: A Proposal to Reconcile Constitutional Practice with Operational Reality*, 14 LEWIS & CLARK L. REV. 687 (2010); Geoffrey S. Corn, *Clinton, Kosovo, and the Final Destruction of the War Powers Resolution*, 42 WM. & MARY L. REV. 1149 (2001); Michael J. Glennon, *Too Far Apart: Repeal the War Powers Resolution*, 50 U. MIAMI L. REV. 17 (1995); Robert F. Turner, *The War Powers Resolution: Unconstitutional, Unnecessary, and Unhelpful*, 17 LOY. L.A. L. REV. 683 (1984); MILLER CTR. OF PUB. AFFAIRS, UNIV. OF VA., NATIONAL WAR POWERS COMMISSION REPORT (2008); THE CONSTITUTION PROJECT, DECIDING TO USE FORCE ABROAD: WAR POWERS IN A SYSTEM OF CHECKS AND BALANCES (2005).

"hostilities" under the statute. In Part V, the "hostilities" analysis is then applied in the cyber context using the Stuxnet[10] computer virus attack in Iran as a test case. The article concludes in Part VI.

II. Section 954 of the NDAA 2012: Military Activities in Cyberspace

On 31 December 2011, Congress passed the National Defense Authorization Act for Fiscal Year 2012. In the section, "Military Activities in Cyberspace," Congress refers to offensive military cyber operations as being subject to the War Powers Resolution.[11] Congress appears to anticipate that some military operations in cyberspace could trigger the provisions of the statute. This assessment of congressional understanding is supported by a plain reading of the text, by the accompanying legislative history, and by the positions expressed in communications between the Senate and the Department of Defense (DoD).

The relevant section of the NDAA 2012 states:

> SEC. 954. MILITARY ACTIVITIES IN CYBERSPACE.
> Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—
> (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and
> (2) the War Powers Resolution (50 U.S.C. 1541 *et seq.*).[12]

A plain reading of this section suggests that the War Powers Resolution may govern certain military operations in cyberspace. While it seems reasonable to direct the Department of Defense to follow the same policy principles and legal regimes when operating cyber capabilities as it does with conventional kinetic capabilities, the reference to the War Powers Resolution is a more provocative statement, as will be explained in this article.

---

[10] THE TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 262 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].
[11] § 954, 125 Stat. at 1551.
[12] *Id.*

The legislative history for the "Military Activities in Cyberspace" section supports the contention that Congress intends to reach military operations in cyberspace with the War Powers Resolution, and offers insight into Congress's rationale. The relevant portion of the Conference Report accompanying the NDAA 2012 addresses use of force and the possible application of the War Powers Resolution:

> The conferees also recognize that in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged. The conferees stress that, *as with any use of force, the War Powers Resolution may apply*.[13]

This piece of legislative history introduces the concept that offensive operations in cyberspace may be considered a use of force, and it is the use of force by the military that may cause the War Powers Resolution to apply. Congress appears to emphasize the military's use of force as the legal trigger for application of the War Powers Resolution to operations in cyberspace. The specific triggering language of the statute will be discussed in more detail in Part III. However, communications between the Senate and the Department of Defense before passage of the NDAA 2012 illustrate the different understandings that the two branches seem to have on this point.

Congress passed the NDAA 2012 shortly after the Department of Defense issued its 2011 "Cyberspace Policy Report" to Congress. This report included responses to thirteen cyber policy questions that had been sent to the Department by the Senate.[14] The final question posed in the report asked, "What constitutes use of force in cyberspace for the purpose of complying with the War Powers [Resolution][?]"[15] The Department of Defense responded, stating:

---

[13] H.R. REP. NO. 112-329, at 686 (2011) (Conf. Rep.) (to accompany H.R. 1540) (emphasis added).

[14] U.S. DEP'T OF DEF. CYBERSPACE POLICY REPORT, A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934, at 1–2 (Nov. 2011), http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf [hereinafter CYBERSPACE POLICY REP.].

[15] *Id.* at 9.

> The requirements of the War Powers Resolution apply to "the introduction of United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."
> Cyber operations might not include the introduction of armed forces personnel into the area of hostilities. Cyber operations may, however, be a component of larger operations that could trigger notification and reporting in accordance with the War Powers Resolution. The Department will continue to assess each of its actions in cyberspace to determine when the requirements of the War Powers Resolution may apply to those actions.[16]

The Department of Defense's answer highlights a difference between congressional understanding and DoD interpretation. The Senate plainly asks *what* constitutes use of force in cyberspace for the purpose of complying with the War Powers Resolution. Phrasing the question in this manner suggests that the Senate is asking the question with the belief that some amount of force in cyberspace would trigger the legislation, and the Senate is asking the DoD to give the parameters of what would constitute that type of action in the cyber domain.

The Department of Defense, however, answers by focusing on the "introduction of armed forces" language in the statute to say that the War Powers Resolution might not apply to cyber operations because those operations might not include the actual introduction of armed forces personnel into the area of hostilities. At the same time, the DoD states that the War Powers Resolution could be triggered when activities in cyberspace are "a component of larger operations."[17] This is presumably because these "larger operations" may include the physical introduction of forces into hostilities.

By focusing on the introduction of personnel and not on the use of force question, the DoD implies that cyber operations on their own could not trigger the statute. This interpretation appears to be at odds with the "Military Activities in Cyberspace" section of the NDAA 2012 and

---

[16] *Id.*
[17] *Id.*

Congress's intent that the language "subject to" the War Powers Resolution has some effect. Congress does not appear to take the view that armed forces personnel must be physically introduced into hostilities before the War Powers Resolution applies to the military activity in question. Instead, Congress appears to focus on whether the military action is a use of force subject to the War Powers Resolution, or in other words, a use of force sufficient to be considered "hostilities" that would trigger the statute.

Congress seems particularly interested in understanding what constitutes a use of force in cyberspace, yet the Department of Defense did not offer an explanation when it was asked in connection to the War Powers Resolution. However, in a previous question in the report, the Department of Defense did offer a method for determining a use of force in cyberspace when asked about acts of war and international law. It is important to note that the term "use of force" in international law has a particular meaning and legal effect, and thus does not carry over directly into an analysis of domestic law. However, a brief review of the Department of Defense's characterization may inform the overall analysis of military operations in cyberspace.

The Senate asked for "[t]he definition or the parameters of what would constitute an act of war in cyberspace and how the laws of war should be applied to military operations in cyberspace."[18] The Department of Defense stated, "Without question, some activities conducted in cyberspace could constitute a use of force, and may as well invoke a state's inherent right to lawful self-defense."[19] The DoD further stated that "a determination of what is a 'threat or use of force' in cyberspace must be made in the context in which the activity occurs, and it involves an analysis by the affected states of the effect and purpose of the actions in question."[20]

The Department of Defense emphasized the importance of context and the effect of cyber operations in making the use of force determination. Looking to the effects of the cyber operations is also highlighted in the "use of force" definition proffered by the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn

---

[18] *Id.*

[19] *Id.* Lawful self-defense refers to a State's rights under Article 51 of the United Nations Charter.

[20] *Id.*

Manual).[21] The Tallinn Manual defines a cyber operation as a use of force "when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[22] These international law explanations of uses of force may be useful when assessing U.S. offensive military operations in cyberspace.

Congress seems to anticipate that some level of military operations in cyberspace could be a use of force sufficient to trigger the War Powers Resolution. This conclusion is supported by a plain reading of section 954 of the NDAA 2012, by the accompanying legislative history, and by the positions expressed in communications between the Senate and the Department of Defense. The executive branch seems to hold a more limited view, according to which stand-alone offensive operations in cyberspace, not involving the physical introduction of armed forces, are not subject to the War Powers Resolution. The positions of these two branches appear to be at odds, with each emphasizing a different portion of the triggering language. The following section examines more deeply the history behind the specific language used in the War Powers Resolution, and how it may have been understood when it was passed in 1973. Part IV turns to the executive branch and its analysis for determining which type of military activities it considers "hostilities" subject to the statute.

III. 1973 Congress and the War Powers Resolution

The War Powers Resolution states that it applies "to the introduction of United States Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and to the continued use of such forces in hostilities or in such situations."[23] This section examines the record of the 1973 Congress to review how the term "hostilities" came to be the operative language of the War Powers Resolution. It explores the War Powers Resolution's legislative history and commentary on that history to discover how "hostilities" may have been understood by the 1973 Congress. It seems the 1973 Congress may have changed the operative language from "armed conflict" to the broader term "hostilities" to present a lower threshold for military activity to trigger the statute, and

---

[21] TALLINN MANUAL, *supra* note 10, at 45.
[22] *Id.*
[23] 50 U.S.C. § 1541(a) (2006).

also to avoid legal implications from international law for use of the term "armed conflict."[24] Legislative history also indicates that the 1973 Congress may have intentionally left the term "hostilities" undefined in recognition of Presidential power and in an effort to give the President flexibility in making the determination of "hostilities" on a case-by-case basis.[25]

The War Powers Resolution was passed over the veto of President Nixon on 7 November 1973.[26] It was enacted "in the wake of the Vietnam War" and represented a bold attempt by Congress to "regulate the President's unilateral use of military force."[27] President Nixon vetoed the War Powers Resolution claiming it was unconstitutional, and no President has expressly conceded its constitutionality since.[28] The stated purpose of the War Powers Resolution, however, is "to fulfill the intent of the framers of the Constitution of the United States and insure that the collective judgment of both the Congress and the President will apply to the introduction of United States Armed Forces into hostilities."[29] The term "hostilities" is repeated throughout the statute, and the determination of the existence of "hostilities" plays a key role in triggering the statute's consultation and reporting requirements, as well as its sixty-day automatic-pullout provision.[30]

The first war powers bill considered by Congress did not refer to "hostilities," but rather the involvement of the Armed Forces in "armed conflict."[31] Throughout the legislative history of the War Powers Resolution, congressmen refer to the "armed conflict" language in

---

[24] *Libya and War Powers: Hearing Before the Comm. on Foreign Relations*, 112th Cong. 24–25 (2011) [hereinafter *Libya and War Powers*] (Sen. Corker); *id.* at 31 (prepared statement of Hon. Harold Koh, Legal Adviser, U.S. Dep't of State, Wash., D.C. [hereinafter Statement of Mr. Koh]).

[25] *War Powers: Hearings Before the Subcomm. on National Security Policy and Scientific Developments of the H. Comm. on Foreign Affairs*, 93d Cong. 22 (1973) [hereinafter *War Powers*] (statement of Hon. Jacob K. Javits, U.S. Senator from the State of N.Y.).

[26] *See* Veto of the War Powers Resolution, 5 PUB. PAPERS 893 (Oct. 24, 1973); RICHARD F. GRIMMETT, CONG. RESEARCH SERV., R41199, THE WAR POWERS RESOLUTION: AFTER THIRTY-SIX YEARS 1 (2010).

[27] CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW 266 n.7 (4th ed. 2011).

[28] STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 307 (5th ed. 2011).

[29] 50 U.S.C. § 1541(a) (2013).

[30] *See id.* §§ 1541–1544.

[31] *War Powers*, *supra* note 25, at 66 (statement of Sen. Eagleton).

various versions of the bill instead of "hostilities."[32] However, it appears that the 1973 Congress may have made the change from "armed conflict" to "hostilities" in the final version to indicate a lower threshold for military action and to avoid legal implications from international law. This interpretation of the legislative history was recently debated by members of Congress and the executive branch during the 2011 Senate hearing *Libya and War Powers*.[33] Referring to the change in language of the War Powers Resolution, Senator Corker stated his opinion that "they tried to make it a lesser level. They started out with 'armed conflict,' and then they used the word 'hostilities.'"[34] Department of State Legal Adviser Harold Koh recognized that the War Powers Resolution House report "suggested that '[t]he word hostilities was substituted for the phrase armed conflict during the subcommittee drafting process because it was considered to be somewhat broader in scope,' but the report provided no clear direction on what either term was understood to mean."[35]

Mr. Koh later explained the change of terms indicating that it had been done to avoid allowing international legal obligations to control the statute:

> Senator Corker had mentioned the House conference report had originally proposed the term "armed conflict." There was an irony in the question which is that "armed conflict" is a term of international law. They deliberately did not import that term into this statute precisely so that international law would not be the controlling factor.[36]

The War Powers Resolution states that it applies "to the introduction of United States Armed Forces into *hostilities*," but the term itself is remarkably unclear. Despite its critical role, "hostilities" was not defined in the text of the War Powers Resolution and has not been defined by Congress in any subsequent legislation or by the courts.[37] There are indications, however, that the 1973 Congress intentionally left the term vague in recognition of Presidential power. The principal sponsor the War Powers Resolution, Senator Jacob K. Javits, was asked at a 1973

---

[32] *See id.* at 70, 77, 78, 84, 200, 229, 293.
[33] *Libya and War Powers*, *supra* note 24, at 13, 24–25.
[34] *Id.* at 24–25.
[35] *Id.* at 13 n.6 (statement of Mr. Koh) (quoting H.R. REP. NO. 93–287, at 7 (1973)).
[36] *Id.* at 31 (statement of Mr. Koh).
[37] *Id.* at 8 (statement of Mr. Koh).

House of Representatives hearing whether the "hostilities" language was problematic because of "the susceptibility of it to different interpretations," making this "a very fuzzy area."[38] Senator Javits acknowledged the vagueness of the language and emphasized that the construction of what is hostilities or the imminent threat of hostilities would be a decision for the President to make.[39] He further clarified that with his bill the President would still have a great deal of power.[40] "No one is trying to denude the President of authority. All that we are claiming is a part in that authority which the Constitution says belongs to Congress."[41]

Again turning to the 2011 *Libya and War Powers* hearing, Mr. Koh acknowledged that "hostilities" is an inherently ambiguous legal standard and stated his opinion that:

> [T]he legislative history of the Resolution makes clear there was no fixed view on exactly what the term "hostilities" would encompass. Members of Congress understood that the term was vague, but specifically declined to give it more concrete meaning, in part to avoid unduly hampering future Presidents by making the Resolution a "one size fits all" straitjacket that would operate mechanically, without regard to particular circumstances.[42]

In 1987, a D.C. District Court gave a similar interpretation stating, "[T]he very absence of a definitional section in the Resolution, coupled with debate suggesting that determinations of 'hostilities' were intended to be political decisions made by the President and Congress, suggest to this Court that fixed legal standards were deliberately omitted from this statutory scheme."[43]

It seems likely that the 1973 Congress intentionally left the term "hostilities" vague in recognition of the powers of the President and in an effort to give flexibility in making a case-by-case "hostilities"

---

[38] *War Powers*, *supra* note 25, at 22 (statement of Hon. Jacob K. Javits, U.S. Sen. from the State of N.Y.).
[39] *Id.* at 21–22.
[40] *Id.* at 22.
[41] *Id.*
[42] *Libya and War Powers*, *supra* note 24, at 13 (statement of Mr. Koh).
[43] Lowry v. Reagan, 676 F. Supp. 333, 340 n.53 (D.D.C. 1987).

determination. The following section focuses the discussion of "hostilities" by exploring how the executive branch has explained which type of military activities it considers to be "hostilities" subject to the War Powers Resolution.

IV. Executive Branch Approach to "Hostilities" Determination

From the beginning, it appears that Congress has largely left the determination of "hostilities" to executive practice.[44] This section will review how the executive branch has explained its determinations in recent years. The executive branch does not consider all situations of U.S. military engagement to be "hostilities" triggering the War Powers Resolution. In determining which type of military activities it considers "hostilities" under the statute, the executive branch appears to make a factual inquiry into the circumstances of the military action and review a set of four limiting factors.

In 1975, Congress asked the executive branch to provide its best understanding of the term "hostilities."[45] Department of State Legal Adviser Monroe Leigh, and Department of Defense General Counsel Martin Hoffmann reported that, as a general matter, the executive branch understood the term "to mean a situation in which units of the U.S. armed forces are actively engaged in exchanges of fire with opposing units of hostile forces."[46] Since the War Powers Resolution was enacted, executive practice has not considered all situations of military engagement to be "hostilities." The executive branch has distinguished "the full military engagements with which the Resolution is primarily concerned" from "sporadic military or paramilitary attacks on our armed forces stationed abroad."[47] As recently as the 2011 military activity in Libya, the executive branch reiterated the distinction between full military encounters and more constrained operations, stating that "intermittent military engagements" do not require the withdrawal of forces under the War Powers Resolution's 60-day rule.[48] According to Mr. Koh, the executive branch has regularly applied this understanding

---

[44] *Libya and War Powers*, *supra* note 24, at 31 (statement of Mr. Koh).
[45] *Id.* at 13–14 (statement of Mr. Koh).
[46] *Id.*
[47] *Id.*
[48] *Id.*

that "hostilities" requires a certain threshold of military activity to trigger the President's obligations under the War Powers Resolution.[49]

In determining whether the minimum threshold of activity has been met, the executive branch appears to understand the "hostilities" determination to require a factual inquiry into the circumstances and conditions of the military action in question.[50] As Mr. Koh explained in 2011, "[S]ince the Resolution's enactment, successive Administrations have thus started from the premise that the term 'hostilities' is 'definable in a meaningful way only in the context of an actual set of facts.'"[51] When looking at the factual circumstances of the proposed action, the executive branch analyzes four factors to determine whether the military activities are likely to rise to the level of "hostilities" for purposes of the War Powers Resolution: whether the mission is limited, whether the risk of escalation is limited, whether the exposure is limited, and whether the choice of military means is narrowly constrained.[52]

While the executive branch has described the discussion of the meaning of "hostilities" between itself and Congress as "ongoing," executive practice seems to reiterate the factors and understanding it supplied to Congress in 1975.[53] As stated by Mr. Koh, in the years since the executive branch reported its understanding of the term "hostilities" to Congress, "the executive branch has repeatedly articulated and applied these foundational understandings."[54] In 2011, the executive branch analyzed the U.S. military strikes in Libya against these four factors to conclude that the operations were "well within the scope of the kinds of activity that in the past have not been deemed to be hostilities for purposes of the War Powers Resolution."[55] It seems fair to state that current executive practice will likely continue to rely on this four-factor inquiry to determine whether a particular military action constitutes "hostilities" under the War Powers Resolution. With this practice in mind, the following section turns the "hostilities" analysis to the cyber domain.

---

[49] *See id.*
[50] *See id.* at 54 (Responses of Legal Adviser Harold Koh to Questions Submitted by Sen. Richard G. Lugar).
[51] *Id.* at 13 (statement of Mr. Koh).
[52] *Id.* at 14; *id.* at 21 (statement of Mr. Koh).
[53] *See id.* at 54 (Additional Material Submitted for the Record, Responses of Legal Advisor Harold Koh to Questions Submitted by Sen. Richard G. Lugar).
[54] *Id.* at 14 (statement of Mr. Koh).
[55] *Id.* at 21 (statement of Mr. Koh).

V. Cyber "Hostilities" Analysis and Stuxnet

This section argues that under the executive branch's existing rubric for determining "hostilities," the President would be highly unlikely to deem stand-alone military operations in cyberspace as "hostilities" for purposes of triggering the War Powers Resolution. Using Stuxnet as a cyber "hostilities" test case, this section applies the executive branch's "hostilities" analysis to the computer virus attack in Iran to reveal the gap that exists between the War Powers Resolution and offensive cyber operations. It is unlikely the President would have considered the operation as triggering any legal obligations under the War Powers Resolution because the Stuxnet mission would have likely been viewed as limited under each of the four factors.

Stuxnet is a computer virus that was reportedly developed by Israel and the United States to attack Iran and set back its nuclear capabilities.[56] It was discovered in 2010, launched between 2007 and 2009, with a variant in operation possibly as early as 2005.[57] Even though the United States has not officially acknowledged its role in the attack,[58] Stuxnet serves as a useful cyber "hostilities" test case because it was a revolutionary offensive cyber-attack[59] and had a wide ranging potential political-strategic effect.

Stuxnet "became known as the first computer software threat that was used as a cyber-weapon."[60] As Dean Turner, a director of Symantec Corporation told Congress, "Stuxnet is a wake-up call to critical

---

[56] *See* Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force,'* WIRED.COM, Mar. 25, 2013, http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/; Ellen Nakashima, *Obama Signs Secret Directive to Help Thwart Cyberattacks*, WASH. POST, Nov. 14, 2012, *available at* http://articles.washingtonpost.com/2012-11-14/world/35505871_1_networks-cyberattacks-defense; Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE INT'L, Aug. 8, 2011, http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

[57] Geoff McDonald, Liam O Murchu, Stephen Doherty & Eric Chien, *Stuxnet 0.5: The Missing Link*, version 1.0, SYMANTEC, Feb. 26, 2013, at 1–2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf.

[58] According to the Conference Report accompanying the NDAA 2012, section 954's reference to offensive military operations in cyberspace includes operations "where the role of the United States Government is not apparent or to be acknowledged." H.R. REP. NO. 112-329, at 686 (2011) (Conf. Rep.) (to accompany H.R. 1540).

[59] *See* McDonald, Murchu, Doherty & Chien, *supra* note 57, at 1.

[60] *Id.*

infrastructure systems around the world. This is the first publicly known threat to target industrial control systems and grants hackers vital control of critical infrastructures such as power plants, dams and chemical facilities."[61] After thorough analysis and reverse engineering, Symantec Corporation declared, "The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries."[62] Stuxnet attacked computers at Iran's Natanz uranium enrichment facility and manipulated its centrifuges to make them self-destruct.[63] It damaged approximately 1,000 centrifuges.[64]

As explained in Part IV, executive practice for determining whether a particular military action constitutes "hostilities" relies on a factual inquiry into the circumstances of a military operation analyzed against a set of four factors: whether the mission is limited, whether the risk of escalation is limited, whether the exposure is limited, and whether the choice of military means is narrowly constrained. It is helpful to keep in mind that these factors originated as an analysis of conventional warfare and, as such, may require a certain amount of translation to the cyber context. Each factor will be analyzed against the Stuxnet attack in turn.

A. Whether the Mission Is Limited

The question of whether or not the mission is limited likely stems from the view that the War Powers Resolution is primarily concerned with "full military engagements"[65] and, therefore, a limited mission may not trigger the statute. The inquiry seems to focus on the nature of the mission, including the role and involvement of U.S. forces. In the case of Libya in 2011, the analysis noted that U.S. forces were playing "a

---

[61] *Securing Critical Infrastructure in the Age of Stuxnet: Hearings before Sen. Comm. on Homeland Security and Governmental Affairs*, 111th Cong. (Nov. 17, 2010) (statement by Dean Turner, Symantec).

[62] Nicolas Falliere, Liam O Murchu & Eric Chien, *W32.Stuxnet Dossier*, version 1.4, SYMANTEC, Feb. 2011, at 2, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[63] Holger Stark, *Stuxnet Virus Opens New Era of Cyber War*, SPIEGEL ONLINE INT'L, Aug. 8, 2011, http://www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html.

[64] Nakashima, *supra* note 56.

[65] *See Libya and War Powers*, *supra* note 24, at 14 (statement of Mr. Koh).

constrained and supporting role" in an operation that was "tailored to a limited purpose."[66]

Under this analysis, the Stuxnet mission would likely be determined "limited" because the role and involvement of U.S. forces appears small and the operation had an arguably limited purpose. The depth of involvement of U.S. forces is not known, but the secrecy involved may imply the use of a small force. Not much is known regarding the official design of the operation. However, one can argue that the results of the attack indicate Stuxnet was a narrow operation by nature and "tailored to a limited purpose." As the Tallinn Manual noted, Stuxnet only damaged specific enemy technical equipment.[67] Stuxnet was "designed to seek out a specific type of industrial process-control system, operating with a particular combination of hardware and software."[68] Data showed there were approximately 100,000 infected hosts by 29 September 2010,[69] with approximately 60% located in Iran,[70] but no discernible damage was reported apart from the Natanz uranium enrichment facility.[71] Stuxnet was "extraordinarily precise in attacking a specific target while inflicting virtually no damage on any other computer systems."[72] With that level of narrow tailoring and apparent limited purpose, it is likely that the executive branch would have considered the Stuxnet mission limited under this prong of the "hostilities" analysis.

B. Whether the Risk of Escalation Is Limited

According to Mr. Koh, the assessment of the risk of escalation focuses on whether or not the U.S. military operation is likely to escalate into a broader conflict.[73] A broad conflict is one characterized by a

---

[66] *Id.*

[67] TALLINN MANUAL, *supra* note 10, at 146.

[68] *Id.* at 170.

[69] Nicolas Falliere, Liam O Murchu & Eric Chien, *W32.Stuxnet Dossier*, version 1.4, SYMANTEC, Feb. 2011, at 5, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[70] *Id.* at 5–6.

[71] John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL J. COMPUTER & INFO. L. 1, 4 (2011).

[72] *Id. See generally* Jeremy Richmond, Note, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INT'L L.J. 842 (2012) (arguing that Stuxnet complied with the law of armed conflict principle of discrimination).

[73] *See Libya and War Powers*, *supra* note 24, at 15 (statement of Mr. Koh).

"large U.S. ground presence, major casualties, sustained active combat, or expanding geographical scope."[74] Like all of the four factors in the "hostilities" analysis, this is an *ex ante* assessment of the risk.

In the case of Stuxnet, the analysis of the risk of escalation would have been made in advance of the operation and likely assessed against Iran's capability of responding to the attack. The operation itself seemed to use few if any U.S. forces and required no active combat. Therefore, whether or not it would escalate into a broader conflict would largely depend on Iran's response. An assessment of another nation's possible response to a military cyber operation would likely review their capability to respond with both kinetic and non-kinetic means. Such an assessment would also likely take into account whether or not the role of the United States was to be acknowledged, as well as other attribution considerations.

With Stuxnet, it is likely that the risk of escalation would have been considered limited. The authors of Stuxnet would have known beforehand that it was designed and tailored to a very particular combination of hardware and software.[75] This could have lessened the estimated risk of escalation because the authors knew that the damage would not expand geographically even if the infection had a large geographical scope.[76] Iran's infected computers were the target, and containing the damage caused by Stuxnet may have lowered the risk of escalation, at least among other nations. Second, there may have been a lower risk of escalation because the attack was so highly cloaked. Stuxnet was not attributed until years after it had been implemented and then discovered.[77] Confidence in the difficulty of attribution and the passage of time between implementation and discovery could lower the risk of escalation. For these reasons, the Stuxnet operation would likely not have been judged as posing a high risk of escalation.

---

[74] *Id.* at 15 (statement of Mr. Koh).

[75] TALLINN MANUAL, *supra* note 10, at 170.

[76] *See* Falliere, Murchu & Chien, *supra* note 69, at 5.

[77] *See* William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0; David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2.

C. Whether the Exposure of U.S. Armed Forces Is Limited

The third factor in the executive branch's "hostilities" analysis asks whether the exposure of the U.S. Armed Forces is limited. This question seems to revolve around U.S. casualties or the threat of significant U.S. casualties.[78] As described by Mr. Koh, a situation of limited exposure could involve "sporadic military or paramilitary attacks on our Armed Forces stationed abroad" in which the overall threat faced by the military is low.[79]

In the case of Stuxnet, the exposure of U.S. Armed Forces personnel in the operation would likely have been viewed as extremely limited. The specific details of the operation are not publically available, but there were no reported casualties associated with the Stuxnet attack[80] or reports of active exchanges of fire with hostile forces. Indeed, in the cyber "hostilities" context, the question of exposure to U.S. Armed Forces is likely to always be assessed as "limited" given the nature of cyber operations. Cyber operations may not require any U.S. forces to enter the geographic area of the attack. The operations may be launched and monitored from inside the United States. The exposure to U.S. forces undertaking offensive operations in cyberspace is likely to be determined significantly limited, particularly in comparison to conventional offensive operations.

D. Whether the Military Means Being Used Are Limited

The final factor in the executive branch's "hostilities" analysis looks to whether the military means being used are limited. This appears to be similar to the first factor in that it compares the proposed military action against a "full military engagement."[81] While the first factor focused on the nature of the mission, this final one emphasizes the type of strikes and the particular military means being used by U.S. forces.[82]

Applied to the Stuxnet attack, the military means used were likely limited. There is no indication that it was a full military engagement.[83]

---

[78] *Libya and War Powers*, *supra* note 24, at 14 (statement of Mr. Koh).
[79] *Id.*
[80] Richardson, *supra* note 71, at 4.
[81] *See Libya and War Powers*, *supra* note 24, at 15 (statement of Mr. Koh).
[82] *See id.* at 16 (statement of Mr. Koh).
[83] *Id.* at 15 (statement of Mr. Koh).

If any U.S. Command was involved, it was likely only U.S. Cyber Command. With the exception of how Stuxnet was possibly introduced to computers that were not connected to the internet, the military activities were likely solely conducted in cyberspace. Stuxnet appears to be an example of an offensive military operation in cyberspace that was unassociated with a larger operation.

In light of the combination of these four factors, it appears likely that if the Stuxnet computer virus attack was a U.S. military operation, the executive branch would not have considered it "hostilities" sufficient to trigger the War Powers Resolution. Under each of the four factors the Stuxnet mission would have been viewed as limited, leading the executive branch to conclude that it did not trigger domestic legal obligations under the statute.

Taking this cyber "hostilities" analysis beyond Stuxnet, military cyber operations in general are unlikely to trigger the War Powers Resolution under the executive branch's existing rubrics. Looking at the four limiting factors together, it seems unlikely that a stand-alone military cyber operation would ever reach the threshold of "hostilities" sufficient to trigger the statute because its mission, military means, and exposure to U.S. forces would always appear extremely limited in comparison to a full military engagement or conventional kinetic military action.

VI. Conclusion

The U.S. military appears to be expanding its offensive cyber capabilities. Congress addressed "Military Activities in Cyberspace" in the NDAA 2012 and suggested a connection to the War Powers Resolution. Congress appears to anticipate that some military operations in cyberspace could trigger the provisions of the statute. The Department of Defense, however, focuses on the lack of introduction of armed forces personnel into the area of hostilities to argue that the War Powers Resolution would not apply to cyber operations. When the executive branch determines which type of military activities it considers to be "hostilities" under the statute, it uses a set of four limiting factors. When this analysis is applied in the cyber context, it illustrates another gap that exists between cyber "hostilities" and the War Powers Resolution. In the case of military cyber operations, the mission, military means, and exposure to U.S. forces would nearly always appear extremely limited,

particularly in comparison to conventional actions or full military engagements. For these reasons, it is unlikely that the executive branch would deem stand-alone offensive military operations in cyberspace as "hostilities" triggering the War Powers Resolution.