THE BLOODY NOSE: 10 U.S.C. § 395

Salahudin Ali*+

The domestic legal regime for regulating military cyberspace operations remains subject to numerous interpretations. 10 U.S.C. § 395, a recent addition to this legal regime, creates a set of notification requirements for sensitive military cyber operations. This paper argues that 10 U.S.C. § 395 will not affect the oversight requirements for certain cyber operations, particularly those that function as cyberspace operational preparation of the environment (COPEs) and occur before traditional kinetic operations.

* Judge Advocate, United States Marine Corps, L.L.M., 2018, Antonin Scalia Law School at George Mason University; J.D., 2011, Lewis & Clark Law School. This article was nominated for the 2019 Dept. of the Navy Office of General Counsel Legal Writing Achievement Award. I'd like to thank Professor Robert Chesney for his thoughts and comments about this article. The comments and opinions in this article are those of the author and are not associated with the Department of Defense or any other government agency. All errors are my own.

+ All sources used herein for the purposes of this article are unclassified or declassified. The author understands that the existence of classified sources may impact the articles analysis.

I. INTRODUCTION

In early January 2018, news outlets began reporting that the United States (U.S.) was considering a preemptive strike against North Korea, dubbed "the bloody nose," in response to multiple ballistic missile tests conducted by North Korea, whose goal was to make missiles capable of reaching the continental U.S.[1] Using a limited military strike, "the bloody nose" would allegedly "batter and humiliate" the North Korean leadership as a response to illegal advances in its weapons programs.[2] Envisioning a successful operation, it is possible that the endeavor would include seizing and securing certain North Korean launch and production sites using America's significant land force already present on the Korean peninsula.[3] There are many ways the operation could be executed, including using the very capable U.S. cyber arsenal to assist in the operation.

---

[1] Abigail Tracey, *With New North Korea Strategy, Trump Administration Flirts with War*, VANITY FAIR, (January 9, 2018), https://www.vanityfair.com/news/2018/01/bloody-nose-north-korea-strategy-trump-administration-flirts-with-war. *See also* Gerald F. Seib, *Amid Signs of a Thaw in North Kora, Tension Bubble Up*, WALL STREET JOURNAL, (January 9, 2018), https://www.wsj.com/articles/amid-signs-of-a-thaw-in-north-korea-tensions-bubble-up-1515427541.

[2] Alex Lockie, *The US is Reportedly Considering a 'Bloody Nose' Attack to Humiliate North Korea - Here's How It Could Go Down*, BUSINESS INSIDER, (January 9, 2018), http://www.businessinsider.com/us-north-korea-bloody-nose-attack-2018-1).

[3] There are an estimated 28,500 troops stationed in South Korea. *See* Mark Landler, *Trump Orders Pentagon to Consider Reducing U.S. Forces in South Korea*, NEW YORK TIMES, (May 3, 2018), https://www.nytimes.com/2018/05/03/world/asia/trump-troops-south-korea.html (last visited June 13, 2018).

Assume that this military operation was conducted using Department of Defense (DoD) military cyberspace[4] capabilities and you are a legal advisor to the agency providing cyber capability support. After the mission is over, you receive an email from a congressional intelligence committee staffer accusing your agency of violating domestic law by failing to notify them about this operation within a reasonable time frame. Your supervisor asks you to begin a draft response, noting that there are certain exceptions to congressional notification for cyberspace operations,[5] but that a new law might have an impact on the current practice.

The answer to the above email may prove more complex than it appears, especially on its application to varying degrees of hostilities. Although there is a domestic legal regime that regulates military cyberspace operations, the plain language found in this regime is open to numerous interpretations.[6] This

[4] GENERAL COUNSEL OF THE DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 16.1.1. (2016) ("Cyberspace may be defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunication networks, computer systems, and embedded processors and controllers."). There may be other definitions, but for our purposes we will use the Department of Defense terminology.

[5] *Id.* at § 16.1.2. ("Cyberspace operations may be understood to be those operations that involve the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyber operations: (1) use cyber capabilities, such as computers, software tools, or networks; and (2) have a primary purpose of achieving objectives or effects in or through cyberspace.") (Internal quotations omitted).

[6] As established in 2009 via MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS (ET. AL.), ESTABLISHMENT OF A SUBORDINATE UNIFIED U.S. CYBER COMMAND UNDER U.S. STRATEGIC COMMAND FOR MILITARY CYBERSPACE OPERATIONS (June 23, 2009), DoD U.S. Cyber Command is subject to the general intelligence oversight regime for operations it conducts. *See* 10 U.S.C. § 167b(e)-(f) ("[t]he commander of the cyber command shall be responsible for, and shall have the authority to conduct, all affairs of such command relating to cyber operations activities . . . .[T]his section does not constitute authority to conduct any activity which, if carried out as an intelligence activity by the Department of Defense, would require a notice to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives under . . . 50 U.S.C. § 3091.") (internal parenthesis omitted); *see also* 50 U.S.C. § § 3091 ("The President shall ensure that the congressional intelligence committees are kept fully and currently informed of the

has been the subject of much commentary focusing on oversight of operations both during hostilities and outside of hostilities, with each concluding in a result dependent on the author's view of national security law.[7]

This article seeks to continue the commentary on the existing oversight regime of military cyberspace operations by examining the impact that the new 10 U.S.C. § 395[8] will have on the covert action statute and its "traditional military activity" exception.[9] Particularly, this article focuses on cyberspace operations used to support traditional kinetic military operations, dubbed "Cyberspace Operational Preparation of the Environment" (COPEs, discussed *infra*).[10] Beginning with Part II

intelligence activities of the United States, including any significant anticipated intelligence activity as required by this subchapter . . . .As used in this section, the term "intelligence activities" includes covert actions as defined in section 3093(e) of this title, and includes financial intelligence activities."); *see also* 50 U.S.C. § 3093 ("[c]overt action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly . . . ").

[7] *See e.g.*, Major Peter C. Combe II, *Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace*, 7 HARV. NAT'L SECURITY J. 526 (2016); Andru E. Wall, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,* 3 HARV. NAT'L SEC. J. 85 (2011); Robert Chesney, *Military-Intelligence Convergence and the Law of the Title 10/50 Debate*, 5 J. NAT'L SECURITY L. & POL'Y 539 (2012) [hereinafter Chesney, 2012]; Robert Chesney, *Computer Network Operations and U.S. Domestic Law: An Overview*, 89 Int'l L. Stud. 217 U.S. Naval War College (2013) [hereinafter Chesney, 2013]; Eric Lorber, *Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?* 15 U. PA. J. CONST. L. 961 (2013); Joshua Kuyers, "*Operational Preparation of the Environment": "Intelligence Activity" or "Covert Action" by Any Other Name?* 4 AM. U. NAT'L L. BR. 21 (2013); Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations,* 111 MICH. L. REV. 423 (2012).

[8] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017), originally codified this law under 10 U.S.C. § 130j, et. seq. The National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018), codified this law in its current form. This article chooses the current form, 10 U.S.C. § 395, for ease of discussion.

[9] 50 U.S.C. § 3093(e) (2018); S. REP NO. 102-85, at 46 (1991), *discussed infra*.

[10] DEP'T OF THE ARMY, CYBERSPACE AND ELECTRONIC WARFARE OPERATIONS, FIELD MANUAL 3-12, at 1-42 (2017) ("Cyberspace [OPE] consists of the non-

of this article, I will discuss the current covert action regime and its applicability to cyberspace operations, and distinguish those actions which are subject to its language from those which are not. In Part III, I will discuss certain typology and tactical considerations of COPE actions. In Part IV, I will examine contemporary attempts to address COPEs by Congress and academia, selectively showing its development as an oversight regime. Part V will examine 10 U.S.C. § 395 and its elements, as well as select examples of its application. Lastly, I will provide my concluding remarks in Part VI. In summary, this article will demonstrate that cyberspace operations which serve as an operational preparation of the environment, and which occur before U.S. military kinetic operations involving U.S. troops, will continue to go unaffected by new developments in the oversight regime.

II. THE ISSUE OF COVERT ACTION AND TRADITIONAL MILITARY ACTIVITIES

10 U.S.C. § 395 is the latest implementation of oversight measures for military cyberspace operations that are used for offensive and defensive purposes conducted outside of the Department of Defense Information Network.[11] This statute attempts to address the ongoing discussion of Department of Defense requirements to keep congressional intelligence and armed services committees fully informed of general intelligence activities and covert military operations.[12] The statute is the

intelligence enabling activities for the purpose of planning and preparing for ensuing military operations . . . .[OPE] in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted [sic] with other United States Government departments and agencies.").

[11] National Defense Authorization Act, *supra* note 8. FIELD MANUAL, *supra* note 10, at 1-28 and 1-37 ("Defensive cyberspace operations are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems . . . ") ("Offensive cyberspace operations are cyberspace operations intended to project power by the application of force in or through cyberspace . . . ").

[12] *See e.g.* 50 U.S.C. §§ 3091-93 (2018); *see, e.g.* Chesney (2012), *supra* note 7, at 611 ("The fundamental problem convergence presents for this framework is embodied by the [OPE] concept described above. When in 2009 [HPSCI] publicly complained about the over expansive application of [OPE], in fact, it

latest attempt at a recalibration between the branches in the exercise of the constitutional war power, Congress's power over spending and military regulation, and the Presidential commander-in-chief power found within the statutory framework. [13] This generally includes congressional recognition of the President's authority to conduct cyberspace operations and Congress's authority to fund and oversee them in accordance with domestic law.[14] In short, as discussed *infra,* it now requires a process of reporting offensive cyber operations to the congressional armed services committees within 48-hours of occurrence, resembling the intelligence oversight regimes vis-à-vis the congressional intelligence committees.[15]

A. Covert Action

Past issues have raised congressional concerns regarding the Department of Defense and it's non-reporting of particular sensitive cyber operations to the congressional committees, which those committees argue is mandated by current statutory reporting requirements.[16] Of primary concern are those operations which may be subject to the covert action statute, 50

was not primarily concerned with circumvention of the covert action system's requirement of presidential authorization.").

[13] U.S. CONST., art. II, § 1 ("The executive [P]ower shall be vested in a President of the United States of America."); U.S. CONST., art. II, § 2 ("The President shall be Commander in Chief of the Army and Navy of the United States . . . "); U.S. CONST., art. I, § 8 ("The Congress shall have the [P]ower to . . . declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water . . . To raise and support Armies, but no Appropriation of Money to that Use shall be for a longer Term than two Years . . . To provide and maintain a Navy . . . To make [R]ules for the [G]overnment and [R]egulation of the land and naval [F]orces . . . ").

[14] 10 U.S.C. § 167b (2017); 10 U.S.C. § 130g (2015); National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81 (Dec. 31, 2011).

[15] 10 U.S.C. § 395(b) (2018); *see also* 50 U.S.C. § 3093 (2018).

[16] Chesney (2012), *supra* note 7, at 611; see also H. R. REP. NO. 111-186, 48-49 (2009) ("The Committee notes with concern the blurred distinction between the intelligence-gathering activities carried out by the Central Intelligence Agency and the clandestine operations of the Department of Defense . . . . [B]ased on recent discussions, the Committee is hopeful that [DOD] will be more fulsome in its reporting.") (Internal parentheses omitted).

U.S.C § 3093.[17] These operations require a detailed written finding and notification by the President to congressional intelligence committees for operations which seek to influence political, economic, or military conditions abroad, where U.S. involvement is intended to be unacknowledged or unapparent.[18] In essence, these operations are intended to be plausibly deniable, meaning an *intent* by the user that the operation not be apparent or acknowledged.[19] Thus, if there is no intent to plausibly deny an operation, then the covert action statute will not apply,[20] but other general oversight measures may apply.[21]

If there is an intent to plausibly deny a given operation, the President must meet certain key statutory requirements.[22] First, the President must make a determination in writing that

---

[17] 50 U.S.C. § 3093(e) (2018) ("'covert action' means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly . . . ") (internal quotations omitted).

[18] 50 U.S.C. § 3093(a)-(h) (2018). Among other things, a written finding and notification must be made by the President indicating necessary foreign policy objectives important to national security, as well as limiting language such as that the covert action does not expand existing authorities, does not involve significant loss of life, does not attempt to influence the U.S. political process, etc. Reports must also be furnished expeditiously to, at minimum (through practice), the "Gang of Eight" of the Intelligence Committees.

[19] 50 U.S.C. § 3093(e) (2018); *see also* National Security Act of 1947, PUB L. NO. 80-253 §§ 2, 102(c), 61 Stat. 495 (1947). Generally, this act provides the intent of Congress to provide a comprehensive program for the future security of the United States, to provide for the establishment of integrated policies and procedures for the departments, agencies, and functions of the Government relating to the national security. It also provided the CIA the ability to perform "such other functions and duties related to intelligence affecting national security . . . (Known as the "fifth function")." (internal parenthesis added). This is widely accepted as the beginning of permissive covert actions. Indeed, these secret and covert actions were interpreted from the authorization to perform "other functions" as all activities which can be plausibly denied. *See* National Security Council Directive on Office of Special Projects Nsc 10/2 (Declassified).

[20] Combe, *supra* note 7, at 534 ("Thus, an unacknowledged military action is not 'covert' if acknowledgement is intended at some point in the future.").

[21] *See*, *e.g.*, 50 U.S.C. §§ 3091- 3092 (2018); these are examples of general intelligence oversight provisions.

[22] 50 U.S.C. § 3093(a)-(h) (2018). I will not list every requirement found in the statute, as it is beyond the scope of this article.

the covert action supports an identifiable foreign policy and national security objective of the United States.[23] Each written finding must describe the covert action, and must include an assurance that the covert action does not violate the Constitution or statutory law; the identity of any third-party funding; a statement that the operation isn't aimed at achieving domestic goals; and the identity of the specific department conducting the operation.[24] Finally, these written findings must be given to the congressional intelligence committees as "soon as possible after such approval and before initiation" of the operation (except as authorized by exceptions within the statute).[25]

Furthermore, the Director of National Intelligence, as well as each department, agency, or other U.S. entity that participates in covert actions, must keep the congressional committee fully and currently informed of their covert actions.[26] This may include specific materials related to the operation.[27] Given the inherent geopolitical and international law risks

[23] 50 U.S.C. § 3093(a) (2018) ("The President may not authorize the conduct of a covert action by departments, agencies, or entities of the United States Government unless the President determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the national security of the United States . . . "). It may be important to note that this statute embodies some constitutional law language found in United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 315-17 (1936) ("In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation.").

[24] *Id.* It is also important to note that, in accordance with Executive Order 12333, no agency except the CIA may conduct covert actions. The DoD may conduct covert actions during a time of war. All other agencies require a determination by the President that they are more likely to achieve a particular objective of the covert action.

[25] 50 U.S.C. § 3093(c)(1)-(5). *Cf.* JAMES BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 152 (Cambridge Press 2007) ("[i]n a side letter to the chairmen of the intelligence committees, President George H.W. Bush undertook as a matter of practice not to withhold notification to the Congress 'beyond a few days' after a finding. This was understood, or interpreted, on the [H]ill as meaning with forty-eight hours. Of course, the 'forty-eight-hour rule' is lore not law, neither is binding on future presidents, but it is a good example of informal constitutional process in intelligence context.").

[26] 50 U.S.C. § 3093(b) (2018).

[27] *Id.*

associated with this type of operation, these requirements are primarily concerned with proper accountability.[28] Should the operation result in the worst possible scenario, this allows Congress to exercise its constitutional funding power to end certain operations by refusing to fund them.[29]

Covert actions should not be confused with clandestine operations; clandestine operations merely assure operational security (i.e. avoidance in getting caught), but lack intent to deny U.S. government involvement.[30] These operations, although

---

[28] Combe, *supra* note 7, at 534-535; *see also* Major Peter Combe II, *The Covert Action Statute: The CIA's Blank Check?* 9 J. NAT'L SECURITY L. & POL'Y 29, 31 (2016). The author argues that domestic law found in the covert action regulatory scheme allows violations of international law which is not effectuated domestically via self-executing treaty or later implementation into domestic statutory law.

[29] *Id; see also* U.S. CONST. art. I, § 8, cl. 1. Indeed, the President must take these oversight measures seriously. Congress has exercised this "power of the purse" in the past. Examples include: Cooper-Church Amendment, Pub. L. No. 91-652, § 2, 84 Stat. 1942 (1970) and the Case-Church Amendment, Pub. L. No. 93-52, 87 Stat. 130 (1973), which sought defund appropriated funds for Vietnam-related activities; Clark-Tunney Amendment to the Arms Export Control Act, Pub. L. No. 94-329, 90 Stat. 729 (1976) (banning covert activities in Angola, it was later repealed in 1985); Hughes-Ryan Amendment to the Foreign Assistance Act of 1961, Pub. L. No. 93-559, 88 Stat. 1725 (1974) (limiting expenditures for covert operations of the CIA to those reported to Congressional committees); and the Boland Amendments of 1982-85, Pub. L. No. 97-377 (prohibiting funding for CIA and DoD operations in Nicaragua), Pub. L. No. 98-215 (limiting amount spent for military purposes in Nicaragua, but prohibiting covert operations funding), Pub. L. No. 98-473 (prohibit funds available to CIA and DoD form being used in Nicaragua for military purposes), and Pub. L. No. 98-83 (excluding military use for funds to be spent in Nicaragua).

[30] JOINT CHIEFS OF STAFF, JOINT PUB. 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS, at 37 (2011) [hereinafter JP 1-02] ("[c]landestine operation — [A]n operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities."); *see also* H. R. REP. NO. 102-06, at 29 (1991) ("The definition of covert action applies only to activities in which the role of the United States Government is not intended to be apparent or acknowledged publicly. Therefore, the definition of 'covert action' does not

secretive in nature, are considered overt operations.[31] Although there may be certain foreign policy and political concerns with their use, clandestine operations do not fall within the scope of the covert action statute, but may be subject to other oversight regimes depending on their use.[32] However, as discussed *infra,* these alternative oversight regimes do not match the level of granular oversight of the covert action statute.[33]

In sum, an operation is covert, or it is not. An action that is plausibly deniable and meets the requirements of the statute will be subject to the statute, including its exceptions.[34] An action that is not plausibly deniable will be subject to other oversight regimes.[35]

B. Traditional Military Activities

Some DoD agencies are subject to the covert action statute insofar as they conduct activities and operations that meet its language (an intent to plausibly deny an operation);

apply to acknowledged United States government activities which are intended to mislead a potential adversary as to the true nature of United States military capabilities, intentions, or operations.").

[31] JP 1-02 at 37; *see also* H.R. REP. NO 102-06, at 29.

[32] In fact, Congress raised this issue in its Intelligence Authorization Act for Fiscal Year 2010, H.R. REP. NO. 111-186, at 49 (2009) ("In the future, if DOD does not meet its obligations to inform the Committee of intelligence activities, the Committee will consider legislative action clarifying the Department's obligation to do so."). This appears to have come true. The National Defense Authorization Act for Fiscal Year 2013 mandated quarterly reporting of DoD cyber operations; this is now codified in 10 U.S.C. § 484 (2018). There also exists a classified briefing which cyberspace operations may be subject to found in 10 U.S.C. § 119 (1987); U.S. Dep't of Def. Dir. 5205.07, SPECIAL ACCESS PROGRAM (SAP) POLICY, Encl. 4 (June 2015), et. al.

[33] *See infra* Part IV.

[34] 50 U.S.C. § 3093(e). Exceptions provide that covert actions do not include those operations whose primary purpose is intelligence, traditional counterintelligence, operational security of U.S. Government programs, or administrative activities; traditional diplomatic activities or military or routine support to such activities; traditional law enforcement activities conducted by United States Government law enforcement agencies or routine support to such activities; or activities to provide routine support to the overt activities or other U.S. Government agencies abroad.

[35] 50 U.S.C. §§ 3091-3092 (2018); H.R. REP. NO. 111-186, at 49 (2009).

DoD has eight intelligence agencies which are subject to oversight by the congressional intelligence and armed forces committees.[36] DoD intelligence agencies operate under both Title 10 U.S.C.,[37] which primarily organizes and gives authorities to the military, and Title 50 U.S.C.,[38] which deals primarily with national security and intelligence. Often the statutes overlap when applied to military operations to the point of being indistinguishable. Congress has made note on occasion, as have those in academia, that there appears to be a "convergence" of these two authorities, making oversight indistinguishable and their independence meaningless.[39] However, the authorities that govern a military operation will often depend upon the purpose and end goal of the operation.[40] As a result, a commander can operate under intelligence authorities for missions in which her primary objective is to acquire or exploit intelligence, and armed forces authorities for missions in which her primary objective is to acquire or exploit intelligence for military purposes.[41]

Some DoD offensive cyberspace operations, although intended not to be acknowledged or apparent, have avoided the process of reporting to the intelligence committees through one key exception: the statute allows for actions consisting of traditional military activities (TMAs) or actions that support

---

[36] DUSTIN KOUBA ET AL., OPERATIONAL LAW HANDBOOK 108 (Dustin Kouba ed., 17th ed. 2017); *see generally* 50 U.S.C. § § 3091-3093 (2018); Exec. Order No. 12333 (1981), *amended by* Exec. Order No. 13284 (2003), Exec. Order 13355 (2004), Exec. Order No. 13740 (2008)(Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the Intelligence commands of each service branch).

[37] 10 U.S.C. §§ 101-18505 (2018).

[38] 50 U.S.C. §§ 1-4705 (2018).

[39] H. R. REP. NO. 111-186, at 48 (2009) ("In categorizing its clandestine activities, [DOD] frequently labels them as 'Operational Preparation of the Environment' to distinguish particular operations as traditional military activities and not as intelligence functions. The Committee observes, though, that overuse of this term has made the distinction all but meaningless.") (internal parentheses omitted); *see also* Chesney (2012), *supra* note 7, at 611.

[40] Covert action requires plausible deniability. If the user does not intend to plausibly deny the action, then the statute will not apply. *See generally,* 50 U.S.C. § 3093 (e) (2018); *Cf.* 50 U.S.C. § 3091(2018), 10 U.S.C. § 167b(e) (2018).

[41] 50 U.S.C. § 3093(e) (2018).

traditional military activities.[42] TMAs are described in the Intelligence Authorization Act of 1991 Senate Report as those activities which "encompass almost every use of uniformed military forces, including actions taken . . . where hostilities with other countries are *imminent* or ongoing."[43] Examples include hostage rescue, terrorist apprehension assistance extraterritorially, and other contingency operations to achieve limited military objectives.[44] From a substantive basis, these operations must be conducted:

> "[b]y military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) *preceding hostilities which are anticipated* (meaning approval has been given by the National Command Authorities for the activities and for operational planning for hostilities) *involving U.S. military forces,* or where such hostilities are ongoing, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly."[45]

Thus, an offensive cyberspace operation may not result in a detailed prompt finding and notification to congressional intelligence committees if, although covert, it is part of a larger military operation that is clear or will be acknowledged. This is not to say that these are wholly unreported. As mentioned above, some activities will always be subject to general intelligence or general armed forces oversight. But, unless use of an offensive cyberspace operation as a TMA reaches outside of an ongoing hostility to constitute its own independent operation, operations conducted during ongoing hostilities cause little concern.[46]

---

[42] *Id.* 50 U.S.C. § 3093(e)(2) (2018).
[43] S. REP. NO. 102-85, at 46 (1991) (emphasis added).
[44] *Id.*
[45] *Id.*
[46] An example of a TMA, which some argue went beyond its bounds, could be the raid to capture (or kill) Osama Bin Laden, code named "NEPTUNE SPEAR". Although primarily operating within Afghanistan, U.S. Special Operations forces crossed the border into Pakistan to conduct the operation, allegedly, without Pakistani knowledge or permission. Due to the language of the 2001 Authorization for the Use of Military Force, questions arose as to whether this

Of concern are those actions which "precede" hostilities that are "anticipated."[47] This was the key issue for offensive cyber operations before the passage of the National Defense Authorization Act for Fiscal Year 2018[48] because of what was perceived as DoD's flexible interpretation of the TMA language.[49] Essentially, any activity which can be shown to have a logical nexus to a future military operation involving U.S. armed forces members anywhere on the globe could be justified as a TMA, so long as the President or Secretary of Defense has planned and approved the activity.[50] The friction point is due to the lack of time constraint requirements as to the "imminence" of the anticipated action, and the lack of clarity as to when the overall operation will be acknowledged (if not apparent).[51] This

truly was a TMA during ongoing operations or an instance which required analysis as a covert action. *See* Pub. L. No. 107-40, § 2(a) 115 Stat. 224 (2001) ("[T]hat the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons."). This somewhat splits TMA analysis to those operations which are related to ongoing hostilities or are preceding one altogether. This may be a moot conversation given the often overlooked fact that President Obama acknowledged the operation, taking the operation out of the covert action oversight framework. *See* Combe, *supra* note 7.

[47] S. REP. NO. 102-85, at 46 (1991).

[48] *See generally* National Defense Authorization Act, *supra* note 8.

[49] *See* H.R. REP. NO. 11-186, 48-49 (2009).

[50] *See* S. REP. NO. 102-85, at 46 (1991) ("It is the [C]ommittee's intent that 'traditional military activities' include activities . . . which approval has been given by National Command Authorities for the activities and for the operational planning for hostilities . . . ") (internal parentheses omitted); Chesney (2012), *supra* note 7, at 600 ("Suffice to say that the nature of the process is to anticipate circumstances that, though potentially quite unlikely, might foreseeably result in an order from the President to use armed force. [F]rom this perspective, the "operational planning" standard included in SSCI's explanation is not nearly as restrictive, in the temporal sense, as the casual reader might assume.").

[51] S. REP. NO. 102-85, at 46 (1991); *see also* Marty Lederman, *Secrecy, Nonacknowledgement, and Yemen*, JUST SECURITY (Feb. 26, 2014) https://www.justsecurity.org/7454/secrecy-nonacknowledgement-yemen/ (last visited, June 13, 2018) ("Let's say that at Time A, the President decides that a particular U.S. activity [say, some sort of use of force in a particular nation] must remain unacknowledged; accordingly, he signs a finding authorizing one or more agencies to undertake that activity as a covert action,

criticism may be unfounded as no language exists in the statute or the legislative history to support it.[52]

There may be other issues concerning the particulars of what constitutes National Command Authority approval: the scope and duration of operational plans, execution orders, etc.; who or what constitutes "armed forces members;" or who is actually in "command" of a mission.[53] I do not mean to minimize the importance of these requirements. In fact, these factors could determine whether the operation may be classified as a TMA to begin with. If these factors are not present, the operation would fall into the category of oversight mandated by the covert action statute due to TMAs containing all elements of covert action, but are an exception nonetheless. However, for purposes of this article, assume that all elements are met, and the only concern is notification to Congress after the TMA is conducted as a COPE.

III. CYBERSPACE OPERATIONAL PREPARATION OF THE ENVIRONMENT

From a tactical standpoint, DoD logically connects TMAs to anticipated operations through a process of "shaping the battlefield."[54] In sum, these are operations conducted to allow

---

and the agencies so authorized begin to engage in unacknowledged uses of force in the nation in question. Then, at Time B, the President decides that U.S. involvement in that nation can now be acknowledged. Subsequent to Time B, does it remain necessary not to acknowledge the actions of the agencies that have been acting pursuant to the earlier covert action finding–a finding that was predicated upon an intent not to acknowledge U.S. involvement? I don't think so. Once the President has determined that nonacknowledgement [sic] of a particular activity is no longer necessary, acknowledgement of the U.S. role in that activity becomes permissible, even as to those actions that are being undertaken pursuant to a covert action finding.").

[52] S. REP. NO. 102-85, at 46.

[53] *See generally* Combe, *supra* note 7, at 541-554. This reference possibly gives the best analysis to date regarding each element of TMA.

[54] LAW OF WAR MANUAL, *supra* note 4, at § 16.1.2.1. ("Cyber operations can be a form of advance force operations, which precede the main effort in an objective area in order to prepare the objective for the main assault. For example, cyber operations may include reconnaissance [e.g., mapping a network], seizure of supporting positions [e.g., securing access to key network systems or nodes], and pre-emplacement of capabilities or weapons [e.g., implanting cyber access

military commanders and decision-makers to accurately plan for major aspects of larger military operations.[55] For example, a cyberspace operation could be used to disrupt an adversary's air defenses during future or incoming airstrikes or the landing of troops on a beachfront in a foreign nation.[56] As mentioned above, these military operations are known as Cyberspace Operational Preparation of the Environment (COPE).[57]

COPEs are currently conducted like any other military operation. Through operational plans, operational orders, and execution orders, COPEs are consistent with the joint planning process and are managed by several internal regulations such as DoD Instructions, Directives, and Executive Orders.[58] A historical precedent exists for these types of tactical operations because

---

tools or malicious code."]); *see also* DEPARTMENT OF DEFENSE CYBER STRATEGY (April 2015) at 14, http://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf ("DoD should be able to use cyber operations to disrupt an adversary's command and control networks, military-related critical infrastructure, and weapons capabilities. As a part of the full range of tools available to the United States, DoD must develop viable cyber options and integrate those options into Departmental plans. DoD will develop cyber capabilities to achieve key security objectives with precision, and to minimize loss of life and destruction of property.").

[55] Joshua Kuyers, *"Operational Preparation of the Environment": "Intelligence Activity" or "Covert Action" by Any Other Name?* 4 AM. UNI. NAT'L SECURITY L. BRIEF, 25 (2013); *see also* Marine Corps Operations, U.S. Marine Corps. § 3-17 (July 26, 2017), https://www.marines.mil/Portals/59/Publications/MCDP%201-0%20W%20CH%201.pdf?ver=2017-09-25-150919-793 ("Shaping incorporates a wide array of functions and capabilities to achieve desired effects and is more than just fires and targeting. It may include, but is not limited to, direct attack, psychological operations, electronic warfare, deception, civil affairs, information management, public affairs, engineer operations, and preventive medical services.").

[56] *Id.*

[57] FIELD MANUAL, *supra* note 10, at 1-10 ("Cyberspace [OPE] consists of the non-intelligence enabling activities for the purpose of planning and preparing for ensuing military operations . . . [OPE] in cyberspace is conducted pursuant to military authorities and must be coordinated and deconflicted [sic] with other United States Government departments and agencies.").

[58] *See generally* LAW OF WAR MANUAL, *supra* note 4; U.S. DEP'T OF DEF., DIR. 2311.01E, DOD LAW OF WAR PROGRAM (May 9, 2006) [hereinafter DoDD 2311.01E]; Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

they have been used throughout recent history and involve a variety of novel technologies to assist in the execution of large, open military operations, which prepare forces for larger and intensified kinetic engagements.[59] These operations permit a force to act overtly through advanced operations, using active and direct measures to develop targets, exploit gaps in enemy systems, and screen follow-on forces.[60] Among other things, COPEs seek to limit the enemy's freedom of action against friendly forces, destroy enemy capabilities, and gain momentum on the battlefield.[61] COPEs should not be confused with cyber exploitation, which seeks to extract otherwise confidential information as opposed to destroying it; such operations are more logically considered primary intelligence activities subject to traditional intelligence oversight.[62]

A COPE can be carried out through an offensive cyberspace operation. Offensive cyberspace operations generally consist of four elements: a vulnerability; access; a payload; and effects.[63] A vulnerability includes aspects of a network which can be compromised by an attacker.[64] Access includes the ability to take advantage of an adversary's system and deliver a payload to

[59] Combe, *supra* note 7, at 550-555. There are some who demand a further element be satisfied for TMAs concerning whether an operation is "traditional" or not. This argument is resoundingly refuted by the legislative record and the way in which the DoD has conducted preparatory actions throughout its history involving advanced technologies. Further discussion of "traditional" nomenclature is beyond the scope of this essay.

[60] FIELD MANUAL, *supra* note 10, at 1-10.

[61] *Id.*

[62] Herb S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 J. of NAT'L SECURITY L. & POL'Y 63, 63 (2010), http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf (last visited 7 June 2018), at 63 (" . . . cyberexploitation [sic] [-] is nondestructive . . . '[C]yberexploitation' [sic] refers to the use of actions and operations – perhaps over an extended period of time – to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks.").

[63] *Id.* at 65-68.

[64] *Id.* at 65. It is of note that the vulnerability can be introduced intentionally or accidently such as a "bug" which opens the door to a system or a zero-day exploit that exists in the operating system that has not been discovered by the operating systems creator.

it.[65] Access is distinguishable by "easy" targets and "difficult" targets; those that involve little effort due to their internet connectivity, and those that require a great deal of effort due to their infrequent connectivity to the internet (think those in which an actor can connect to a computer via an unprotected network, as opposed to those which have adequate malware security).[66] They are also distinguishable by those that require remote access or close access (for example, someone accessing your computer while you're using the local coffee shop's Wi-Fi-network; or accessing through the hardware supply-chain, i.e. accessing through spare parts sold independently to be combined in some final product).[67] Payloads are things that can be done once a vulnerability has been exploited, and includes many types of viruses and malware.[68] Lastly, effects includes any attributes caused to be lost by the attack.[69] They include loss of integrity, authenticity, and availability of an operating system; they are impacts (usually negative) that were not present before the payload was delivered.[70]

The tactical impact of these technical means are felt across cyberspace, defined by DoD as "global," including on interdependent networks of technology infrastructures, the internet, telecommunications networks, computer systems, and embedded processors and controllers.[71] DoD divides cyberspace into layers in which offensive cyberspace operations are felt;

---

[65] *Id*. at 66.
[66] *Id.*
[67] *Id*. at 66-67. The author classifies them as "Remote access" targets and "Close access" targets. "Remote access" being those which are compromised at a distance via the internet, dial up modem, or wireless network. "Close access" being those are compromised through local installation hardware or software functionality near a computer network or network of interest. An example of this could be a supply-chain vulnerability ordered from an adversary's private sector company.
[68] *Id*. at 67.
[69] *Id* at 67-68.
[70] *Id.*
[71] LAW OF WAR MANUAL, *supra* note 4, at 16.1.1 ("Cyberspace may be defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunication networks, computer systems, and embedded processors and controllers."); *e.g.*, DoDD 2311.01E.

those layers consist of the physical network, the logical network, and the cyber-persona.[72] Each layer is affected differently for the primary purpose of achieving objectives in or through cyberspace.[73] The purpose is to degrade, disrupt, deny, destroy, or manipulate aspects of an operating system to cause an intended effect.[74] By using these technical measures to achieve

[72] FIELD MANUAL, *supra* note 10, at 1-13 – 1-14 ("The physical network layer includes geographic and physical network components. The geographic component is the physical location of elements of the network. The physical network component includes all the physical equipment associated with links (wired, wireless, and optical) and the physical connectors that support the transfer of code and data on the networks and nodes."); ("The logical network layer consists of the components of the network that are related to one another in ways that are abstracted from the physical network. For instance, nodes in the physical layer may logically relate to one another to form entities in cyberspace that are not tied to a specific node, path, or individual. Web sites hosted on servers in multiple physical locations where content can be accessed through a single uniform resource locator or web address provide another example."); and ("The cyber-persona layer is an abstraction of the logical network, and it uses the rules of the logical network layer to develop a digital representation of an individual or entity identity in cyberspace consists of the people who actually use the network and therefore have one or more identities that can be identified, attributed, and acted upon. These identities may include e-mail addresses, social networking identities, other web forum identities, computer internet protocol addresses, and cell phone numbers.").

[73] LAW OF WAR MANUAL, *supra* note 4, at 16.1.2.

[74] *Id.* at 16.1.2.1 ("Cyber operations include those operations that use computers to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."); *see also* FIELD MANUAL, *supra* note 10, at 1-10 - 1-11 ("Joint cyberspace operations doctrine describes cyberspace actions. Cyberspace actions at the joint level require creating various direct denial effects in cyberspace [degradation, disruption, or destruction]. Joint cyberspace operations doctrine also explains that manipulation leads to denial [hidden or manifesting] in any Domain."); and ("These specific actions are—**Deny**. To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents enemy or adversary use of resources. **Degrade**. To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified. **Disrupt**. To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent. **Destroy**. To deny permanently, completely, and irreparably (time and amount are both maximized) access to, or operation of, a target. **Manipulate**. To control or change the enemy or

intended effects in an adversary's cyberspace, the expectation is that the overall tactical military operation will improve.

IV. ATTEMPTED SOLUTIONS: LEGISLATION AND SELECTED ACADEMIA

A. Legislation

Due to the ease by which these operations may be indexed as preparatory actions exempt from covert action reporting, and the obvious oversight and foreign policy concerns of congressional committees, multiple attempts have been made to limit TMAs.[75] One of the first noted attempts to address the issue came in the Intelligence Authorization Act for Fiscal Year 2010 when Congress gave a "warning shot" to DoD that a new shift in legal oversight was impending, noting that, "[I]n the future, if [DoD] does not meet its obligations to inform the committee of intelligence activities, the committee will consider legislative action clarifying the department's obligation to do so."[76] The committee's issue with the DoD legal analysis is that clandestine operations (those with no intent to be unapparent or unacknowledged, but focus on operational security) labeled as TMAs do not require congressional reporting—this was perceived by Congress as abstractions to justify theoretical and distant military operations.[77] Indeed, Congress had already become sensitive to the possibility that TMAs were producing oversight gaps, and had begun passing National Defense Authorization Act provisions that dealt with different types of special operations (including unmanned aerial vehicle strikes).[78]

---

adversary's information, information systems, and/or networks in a manner that supports the commander's objectives.").

[75] *See supra* note 32 and accompanying text.

[76] PERMANENT SELECT COMM. ON INTELLIGENCE, H.R. REP. NO. 111-186, Intelligence Authorization Act for Fiscal Year 2010, at 49 (2009).

[77] *Id.*

[78] *See* Robert Chesney, *Important New Oversight Legislation for Military Kill/Capture Outside Afghanistan,* LAWFARE (May 9, 2013, 12:24 AM),https://www.lawfareblog.com/important-new-oversight-legislation-military-killcapture-outside-afghanistan; *see also* Robert Chesney, *Oversight of DoD Kill-Capture Missions Outside Theaters of Major Hostilities: What May Change Under the Next NDAA?* LAWFARE (May 20, 2016, 4:02 PM),

To Congress, these operations posed the same risks as covert actions. Hence, they should be subject to the same type of reporting mechanism as covert actions.[79]

A second noted congressional attempt at limiting this use of TMAs came in the National Defense Authorization Act for Fiscal Year 2012. Congress made clear that it recognizes the President's authority to conduct offensive cyber operations upon his order, but that these operations are subject to domestic and international legal regimes, including the War Powers Resolution (which will be important to the discussion below).[80] However, this language did not provide the level of detail needed to potentially force reporting to congressional intelligence committees; in fact, it was unclear if it required reporting to Congress at all.[81] As opposed to fixing the issue of non-reporting, it may have further convoluted the conversation about cyberspace TMA operations and their subjectivity to congressional committee reporting by raising more questions than answers.[82]

---

https://www.lawfareblog.com/oversight-dod-kill-capture-missions-outside-theaters-major-hostilities-what-may-change-under-next; Robert Chesney, *Expanding Congressional Oversight of Kill/Capture Ops Conducted by the Military: Section 1036 of the NDAA*, LAWFARE (December 8, 2016, 6:25 PM), https://www.lawfareblog.com/expanding-congressional-oversight-killcapture-ops-conducted-military-section-1036-ndaa.

[79] *See supra* note 76.

[80] Pub. L. No. 112-81 (Dec. 31, 2011) ("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.") (Internal parentheses omitted).

[81] Robert Chesney, *Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate*, LAWFARE (Dec. 14, 2011, 10:17 PM), https://www.lawfareblog.com/offensive-cyberspace-operations-ndaa-and-title-10-title-50-debate ("[t]here is a reference to the [WPR], which has a similarly unclear effect . . . [W]hich raises the question whether there isn't some better way to ensure some amount of legislative awareness of such operations.").

[82] *Id.* In response to the reports explanatory statement regarding TMAs and offensive cyber operations, the author comments, "That is not the clearest language ever. It seems to me, however, that this is meant to overcome any

Another noted attempt at limiting non-reporting of offensive cyberspace operations as TMAs came in the National Defense Act for Fiscal Year 2013.[83] This requirement provided that offensive and significant defensive military cyberspace operations carried out by DoD must be reported quarterly to the congressional armed services committees.[84] This piece of legislation was an advancement of congressional efforts to rain in unreported TMA usage for offensive cyberspace operations, but again, it lacked the level of detail and requirement of timeliness of the covert action statute. However, in Section 940 of the act, Congress posed the question of how a single commander can conduct both "overt, though clandestine, cyber operations under title 10, United States Code, and [serve] as the head of an element of the intelligence community that conducts covert cyber operations . . . in a manner that affords deniability to the U.S . . . ."[85] This language may note the frustration of the very body that drafts oversight and appropriations for DoD activities, and was perhaps a foretelling of what was to come, depending upon which legal rationale DoD chose as its answer. That is, a reporting system that would require the level of detail and oversight desired by congressional committees over military cyberspace operations.[86]

It is important to note that this progression of oversight for new and novel technologies applied to national defense is nothing new, but this oversight has often been challenging for Congress. Professors David P. Auerswald and Colton C. Campbell

argument that OCOs cannot qualify as 'traditional military activities' simply because of the novelty of their nature and the technologies involved."

[83] National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, 126 Stat. 1632 (2013) [hereinafter 2013 NDAA], amend. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017); 10 U.S.C. § 484(a) (2018).

[84] 10 U.S.C. § 484(a) (2018).

[85] 2013 NDAA, Pub. L. No. 112-239 § 940(4)(D)(i) (2013).

[86] DoD intelligence agency commanders operate under both Title 10 and 50 U.S.C. Specific regulatory obligation is determined by the facts of the operation. For example, if the action is primarily meant for intelligence gathering, both titles will apply. If the action was meant to be covert, only title 50 would apply. Lastly, if the action is an overt offensive cyberspace operation, Title 10 would primarily apply.

note in their book, *Congress and the Politics of National Security*, "[E]fforts by lawmakers in Congress to maintain accountability over intelligence agencies . . . has proven difficult and has often *failed*."[87] Professor Auerswald and Campbell further provide that throughout U.S. history, phases in time have dictated the attitude that Congress brings to the oversight conversation.[88] These phases in time are comprised of the era of trust (1784-1974), the era of uneasy partnership (1974-1986), the era of distrust (1986-1991), the era of partisan advocacy (1991-2001), and the current era of ambivalence (2001-present).[89] Phases of action exist within each era of time.[90] Eras of action comprise of "low-intensity patrolling," "shock" (or failure and scandal), "firefighting" (passage of new legislation), and "high-intensity patrolling" (enforcement of new legislation) which exists within each era as reference points.[91]

The era of trust is considered a time when the U.S. valued efficiency over oversight, and intelligence was used to fight America's enemies under the assumption that agencies would have to be trusted in performing their duties without concern that their power would be abused.[92] Indeed, this was the case for

[87] Loch K. Johnson, Congress and Intelligence, *in* CONGRESS AND THE POLITICS OF NATIONAL SECURITY 121 (David P. Auerswald & Colton C. Campbell eds., Cambridge University Press 2012) (emphasis added).
[88] *Id.* at 121-137.
[89] *Id.*
[90] *Id.* at 130-37.
[91] *Id.*
[92] *Id.* at 122-23. As the authors provided, this era was not wholly unchecked. Many intelligence actions consisted of approval from the President or other national command authorities, and the Central Intelligence Agency would report from time-to-time its operations to Congress. There were also instances of inquiry by Congress for embarrassing intelligence failures such as the Bay of Pigs, the U-2 incident shot down over the Soviet Union, and CIA domestic operations conducted by the National Student Association. But this era may be summarized as an era which led to new and expansive intelligence authorizations beginning with the National Security Act of 1947 establishing the modern American Intelligence Community.

almost two centuries of operation against American adversaries.[93]

The era of uneasy partnership comprised of a series of committee formations known as the Church Committee and Pike Committee to explore intelligence domestic and foreign intelligence abuses by the government as a response to *New York Times* reports.[94] The Church and Pike Committee found the news reports valid, and eventually discovered deep intelligence abuses by American intelligence agencies conducting secret operations and covert actions.[95] The era coalesced with the passage of the Hughes-Ryan Act,[96] detailing the first instance where the President must provide his national security justification for actions that are not routine intelligence operations.[97] This era also formalized Congress's role in intelligence oversight of all intelligence activity (to include DoD) with the establishment of both congressional intelligence committees; these committees could exercise the "power of the

---

[93] David P. Auerswald and Colton C. Campbell, CONGRESS AND THE POLITICS OF NATIONAL SECURITY 122-23 (Cambridge University Press, 2012).

[94] *Id.* at 123-27.

[95] *Id.* The authors mention covert operations conducted against Chile's democratically elected Allende's government; CIA's operations domestically such as OPERATION CHOAS; ARMY and NSA intelligence operations dubbed OPERATION SHAMROCK and MINARET; and the infamous FBI program, COINTELPRO.

[96] "(a) No funds appropriated under the authority of this or any other Act may be expended by or on behalf of the Central Intelligence Agency for operations in foreign countries, other than activities intended solely for obtaining necessary intelligence, unless and until the President finds that each such operation is important to the national security of the United States and reports, in a timely fashion, a description and scope of such operation to the appropriate committees of the Congress, including the Committee on Foreign Relations of the United States Senate and the Committee on Foreign Affairs of the United States House of Representatives. (b) The provisions of subsection (a) of this section shall not apply during military operations initiated by the United States under a declaration of war approved by the Congress or an exercise of powers by the President under the War Powers Resolution." Foreign Assistance Act of 1974, Pub. L. No. 93-559, 88 Stat. 1795 (1974).

[97] *Id.* These actions now required a finding based upon language found in the *Curtiss-Wright* decision signifying a significant foreign affairs issue based upon the Presidents sole representative with foreign nations' role. *Curtiss-Wright*, 299 U.S. 304 (1936).

purse" to check executive branch operations as an exercise of its constitutional war power.[98]

The era of distrust can be summarized as an era that responded to continued intelligence abuses in the face of the new formalized oversight created during the previous eras. Here, as a response to direct bypass of congressional oversight, intelligence abuses, and military-intelligence failures, Congress established more pointed intelligence oversight found in the Hughes-Ryan Act,[99] the Inspector General Act of 1989,[100] the Goldwater-Nichols Act,[101] and the Intelligence Authorization Act of 1991.[102] These pieces of legislation established meaningful oversight, control, and clarification of responsibilities and authorization in conducting intelligence activities.

The eras of partisan advocacy and ambivalence are unique. Congress sought to use the established oversight bodies

[98] House Permanent Select Committee On Intelligence (HPSCI), H. Res. 658, 95th Cong. (1978) (" . . . [e]stablishing the Permanent Select Committee on Intelligence . . . Requires the Select Committee to obtain an annual report from the Directors of the Central Intelligence Agency and the Federal Bureau of Investigation and the Secretaries of State of Defense reviewing the intelligence and intelligence-related activities of the agency or department and of foreign countries directed at the United States."); and Senate Select Committee On Intelligence (SSCI), S. Res. 400, 95th Cong. (1976) ("States that the purpose of this resolution is to establish the Senate Select Committee on Intelligence. Requires such Committee to make every effort to assure that the appropriate departments and agencies provide informed and timely intelligence necessary for the executive and legislative branches to make sound decisions on national security.").

[99] *Id.*

[100] Intelligence Authorization Act for Fiscal Year 1990, Pub. L. No. 101-193, 103 Stat. 1701 (1989).

[101] Goldwater-Nichols Department of Defense Reorganization Act of 1986, Pub. L. No. 99-433, 100 Stat. 992 (1986) ("An [A]ct To reorganize the Department of Defense and strengthen civilian authority in the Department of Defense, to improve the military advice provided to the President, the National Security Council, and the Secretary of Defense, to place clear responsibility on the commanders of the unified and specified combatant commands for the accomplishment of missions assigned to those commands and ensure that the authority of those commanders is fully commensurate with that responsibility . . . ").

[102] Intelligence Authorization Act for Fiscal Year 1991, Pub. L. No. 102-88, 105 Stat. 429 (1991).

for political expediency against whichever opposite political party was in office.[103] However, after the 9/11 attacks, these bodies rallied behind intelligence communities giving a swarm of new flexibility to fight new and asymmetrical enemies of the state.[104] Although unclear exactly which classification the current era should be given, revelations of mass data collection and cyber capabilities may have opened a new front where trust, distrust, partnership, and political advocacy are all present.[105] The recent passage of the FISA Amendments Reauthorization Act of 2017[106], the Cloud Act,[107] and of course, 10 U.S.C. § 395,[108] may yield an era of increased oversight.

What can be observed from recent attempts, as well as those throughout history, is that a new trend of increased efforts in oversight continues to lag behind increasingly fast technological advancements in national security practice. As related to offensive cyberspace operations, the development of oversight is slow and compounding. For TMAs and offensive cyberspace operations, Congress slowly began to tip the balance back toward oversight to avoid the same issues as described by the eras of intelligence oversight involving a lack of awareness and political willpower.

---

[103] Lin, *supra* note 62, at 128.
[104] *Id.* at 128-29.
[105] *See e.g.,* American Civil Liberties Union Foundation, Privacy and Surveillance Section https://www.aclu.org/issues/national-security/privacy-and-surveillance/nsa-surveillance (last visited May 13, 2018); Casey Burgat and Daniel Schuman, *The Cautionary tale of the House Intelligence Committee's recent failures.* THE BROOKINGS INSTITUTE (June 8, 2018), https://www.brookings.edu/blog/fixgov/2018/04/04/the-cautionary-tale-of-the-house-intelligence-committees-recent-failures/ (last visited, June 8, 2018).
[106] FISA Amendments Reauthorization Act of 2017, S. 139 (2017) (containing enhanced intelligence collection, safeguards, and oversight).
[107] Clarifying Lawful Overseas Use of Data Act (CLOUD), H.R. 4943, 115th Cong. (2018) (amending the Stored Communications Act and its applicability to deal with cloud computing practices of decentralized data storage).
[108] 10 U.S.C. § 395 (2016) (creating a parallel findings and reporting mechanism for cyber operations that are not captured by 10 U.S.C. § 3093).

B. Selected Academia

Starting in 2009, offensive cyberspace operations as applied to the domestic intelligence oversight regime increasingly became *en vogue*. With the release of the *National Research Council Report, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,"*[109] a new focus emerged of deciding exactly how these offensive cyberspace operations would be categorized.[110] The report is lengthy (367 pages if one includes the appendix), but provides probably the best scope and breadth of offensive cyberspace analysis available by including sections on nomenclature, typology, technological aspects, and classification of techniques. In Part II and III of the report, attention is given to the development of (what was then) new DoD doctrine on use of offensive cyberspace operations, legislation to deal with emerging lack of oversight, intelligence community uses, and the applicability of offensive cyberspace operations to domestic law,[111] most notably TMAs.[112] The report, in sum, highlighted issues and questions as to use of offensive cyberspace operations. The report concluded with multiple findings which may have served as a call to action for a proper legal regime; select portions provided that the existing legal framework of the time was ill-equipped to deal with the technology, and that Congress had a substantial role to play in its development.[113]

In 2011, Andru Wall wrote in his article, *Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations,*

[109] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Research Council (2009).
[110] *Id*., e.g. Part II, at 159-236; and Part III, at 237-333.
[111] *Id.*
[112] *Id.* at 284-85 ("Given this legal environment, it is not surprising that executive branch decision makers have adopted an expansive view of actions that might be considered traditional military activities, and that includes actions that have a very direct military effect on potential military adversaries—even if actions would constitute covert action if undertaken by the intelligence community.").
[113] *Id.* at 5-6.

Intelligence Activities & Covert Action,[114] that due to modern warfare's close integration of military and intelligence forces, both Title 10 and 50 of the United States Code should be viewed as mutually supporting authorities.[115] The article notably provides clarity as to which arguments are grounded in appropriate legal analysis and which arguments are more appropriate for policy and political discussion.[116] Another key point of the article is that it simplifies notions that secretive operations must be conducted under one authority or another. Rather, these operations can overlap, given the TMA exception to the covert action statute, regardless of congressional attempts to redefine these operations without the passage of new legislation.[117] He notes:

> "Congress's failure to provide necessary interagency authorities and budget authorizations threatens [our] ability to prevent and wage warfare. Congress's stubborn insistence that military and intelligence activities inhabit separate worlds casts a pall of illegitimacy over interagency support, as well as unconventional and cyber warfare. The U.S. military and intelligence agencies work together more closely than perhaps at any time in American history, yet Congressional oversight and statutory authorities sadly remain mired in an obsolete paradigm."[118]

Conclusively, this article pinpoints what the legal discussion at that time entailed, as well as appropriate criticism, challenging legislators to address the issue by creating proper legal oversight regimes.

---

[114] Wall, *supra* note 7.
[115] *Id.* at 85 ("The Secretary of Defense possesses authorities under Title 10 and Title 50 and is best suited to lead US government operations against external unconventional and cyber threats. Titles 10 and 50 create mutually supporting, not mutually exclusive, authorities.").
[116] *Id.* at 88-92. The author sums these up as arguments about appropriate roles, missions, budgets, and transparency of executive branch operations.
[117] *Id.* at 141.
[118] *Id.*

Moreover, 2012 and 2013 brought two articles from Professor Robert Chesney specifically dealing with offensive cyber operations: "*Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate"* and "*Computer Network Operations and U.S. Domestic Law: An Overview."*[119] In their relevant portions, both articles explore offensive cyberspace operations as TMAs, many of which are considered COPEs when used for shaping operations, and their applicability to the covert action statute.[120] As related to the issues of offensive cyber operation and congressional oversight, the first article explores the history of covert actions and TMAs, then concludes that a new legal regime could be established by the congressional intelligence and armed services committees that resembles the covert action statute's reporting regime.[121] The second article, dealing exclusively with offensive cyber operations, pointedly constructs the question of offensive cyber operations' subjectivity to Congressional reporting mechanisms found in the covert action statute regime.[122] The question was ultimately answered by Professor Chesney, who provided, "[A]t the end of the day, however, the fact remains that categorization as TMA or routine support to TMA removes the statutory requirement of relatively granular reporting to Congress (under the covert action statute)."[123]

Both conclusions are reached due to Professor Chesney's analysis of TMA factors, mainly, his analysis under the

[119] Chesney (2013), *supra* note 7; Chesney (2012), *supra* note 7.
[120] Chesney (2013), *supra* note 7, at 219-23; Chesney (2012), *supra* note 7, at 607-16.
[121] Chesney (2012), *supra* note 7, at 615 ("Legislation could and probably should establish a mechanism for reporting such activities to [SASC] and [HASC], modeled on the [Gang of Eight]").
[122] Chesney (2013), *supra* note 7, at 219 ("The issue with respect to congressional oversight is whether the executive branch must give notice of a given CNO (or programmatic series of CNOs) to (i) the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (collectively, the Intelligence Committees), (ii) to the Senate Armed Services Committee and the House Armed Services Committee (collectively, the Armed Services Committees), (iii) to both pairs or (iv) to none of the above.").
[123] *Id.* at 223 (parenthesis added).

"preceding" and "anticipated" hostility factor of TMAs.[124] While Congress (as Andru Wall mentioned above) attempted to redefine elements of TMA without legislation, Professor Chesney notes from the legislative history that, as long as operational planning has been approved by the appropriate authorities, "the 'operational planning' standard . . . is not nearly as restrictive, in the temporal sense, as the casual reader might assume."[125] Other factors are analyzed within the two articles, but the temporal and geographic scope were important points for offensive cyberspace operation analysis. In the end, as demonstrated by each article, as well as legislative attempts described in Part IV.A, calls for reform and legislation would be best served by closing this gap.

Lastly is Major Peter Combe's 2016 article, *Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace*.[126] In this article, Major Combe applies the TMA framework to military information and offensive cyberspace operations. Major Combe examines each requirement for a TMA, arguing that temporal and geographic concerns for offensive cyberspace operations, such as TMAs, may be remedied by a number of tests: (1) for operations occurring inside an area of current military operation (current hostility); and (2) for operations occurring outside of an area of current military operations.[127] Furthermore, Major Combe argues that intent for acknowledgement and apparentness should be documented, as well as improved reporting to the armed services committees to close the gap of unawareness by the intelligence committees.[128] He ultimately concludes that the current regime is outdated in light of statutory convergence and cyberspace operations.[129] But, he also concludes that a focus on geographic location of operations, as

[124] Chesney (2013), *supra* note 7, at 221; Chesney (2012), *supra* note 7, at 612.
[125] Chesney (2012), *supra* note 7, at 600.
[126] Combe, *supra* note 7.
[127] *Id.* at 566-74.
[128] *Id.* at 573.
[129] *Id.* at 574.

related to military operations, as well as appropriate documentation, may remedy concerns.[130]

What can be summarized from this selected academia is that the salient issue of concern involved addressing ambiguous and archaic language found in the oversight regime. Potential gaps and concerns were identified, appropriate focus to law was advised, and analysis and recommendations for the future were forwarded. The issue appeared clear, but Congress took pace to finally craft an oversight regime to deal with the issue instead of projecting its concerns within years of authorization legislation.

V. CURRENT SOLUTION: 10 U.S.C. § 395

Enter 10 U.S.C. § 395. Finally addressing the issue of DoD COPE usage, Congress presented, and the President signed, the National Defense Authorization Act for Fiscal Year 2018.[131] To recall, this legislation requires the Secretary of Defense to "promptly" submit to the congressional armed services committees a notice in writing of any "Sensitive Military Cyber Operation (SMCOs)" within 48 hours of occurrence.[132] In its relevant part, SMCOs are defined as:

> "Sec. (c): . . . [a]n action . . . that— (A) is carried out by the armed forces of the United States; and (B) is intended to cause cyber effects outside of a geographic location— (i) where the armed forces of the United States are involved in hostilities (*as that term is used in section 1543 of title 50, United States Code)*; or (ii) with respect to which hostilities have been declared by the United States."[133]

Offensive cyberspace and defensive actions outside of the Department of Defense Network are covered.[134] There are notable exceptions to this statute.[135] Training exercises

---

[130] *Id.* at 574-76.
[131] Pub. L. No. 115-91, 131 Stat. 1283 (2017). Codified as 10 U.S.C. § 130j, now codified as 10 U.S.C. § 395. *See supra* note 8 and accompanying text.
[132] 10 U.S.C. § 395(a) (2018).
[133] *Id. § 395(c).*
[134] *See id.* § 395(c)(2).
[135] *Id.* § 395(d).

conducted with the consent of all nations affected by the cyber operation, as well as *covert actions*, are not subject to the statute.[136] Additionally, the statute explicitly states that it is not to be construed as a grant of new authority to alter or affect the War Powers Resolution,[137] the Authorization for Use of Military Force,[138] or any requirement under the National Security Act of 1947.[139] This indicates that this statute is a separate procedural regime that complements, but does not replace, existing responsibilities under other legal oversight regimes for offensive cyberspace operations.[140]

Professor Robert Chesney noted in a 2017 article, *Offensive Cyberspace Operations, the NDAA, and the Title 10-Title 50 Debate,* that this new statute appears to "pick up some but not all . . . traditional military activities (as related to offensive and defensive cyber operations)," which were previously unreported under the covert action statute.[141] This is true in some sense, especially considering those offensive cyberspace operations which are conducted completely independent of a geographical location where there will be no conceivable kinetic military operation involving U.S. troops. Supposedly, Congress would have previous notification of a situation under the current statutory regime for those TMAs conducted pursuant to ongoing hostilities.[142] COPEs, which lack operational plans or execution orders as proof of the existence of a future kinetic military operation that will likely involve U.S.

---

[136] *Id.*

[137] 50 U.S.C. § 1541, *et. seq*. (1973).

[138] Authorization for Use of Military Force Against Those Responsible for Attacks Launched Against the United States on Sept. 11, 2001, Pub. L. No. 107-40, 115 Stat. 224 (2001).

[139] 50 U.S.C. § 3001, *et. seq*. (1947).

[140] 10 U.S.C. § 395(e) ("Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect the War Powers Resolution, [the] Authorization for Use of Military Force, or any requirement under the National Security Act of 1947.") (internal parentheses omitted).

[141] Robert Chesney, *Offensive Cyberspace Operations, the NDAA, and the Title 10-Tile 50 Debate*, LAWFARE (Dec. 14, 2011), https://www.lawfareblog.com/offensive-cyberspace-operations-ndaa-and-title-10-title-50-debate (last visited, June 13, 2018).

[142] 50 U.S.C. § 1541(a) (2018).

service members in a specific geographic location, will find it difficult to justify the existence of such for purposes of an exception to this new statute. However, a closer examination of the language may prove this new statute is not as strict as originally thought.

To start, a COPE conducted as a TMA would meet most of the elements included in 10 U.S.C. § 395. That is, they are conducted by U.S. armed forces (by its members and commanded by a military commander) and cause any effect on adversary computer networks (degrading, denying, or disrupting the physical, logical, or persona layer of an adversary's computer network system) a contingency to allowing further military action .[143] The plain language of "effects" would also appear to take SMCOs out of a general intelligence collection regime, as effect differs from that of "exploitation."[144] The foreseeable issue will be defining "hostilities" for purposes of reporting, as the term is used in the statute. The statute provides that "hostilities" is to be used as it is in the War Powers Resolution,[145] but we must not forget the term's relationship within the TMA legislative language, which indicates that anticipated imminent hostilities are "hostilities," too.[146] Thus far, most scholarship focuses on a linear-normative approach, addressing mainly oversight of COPEs conducted during ongoing hostilities or completely independent of ongoing hostilities.[147] There remains a gap for those operations conducted within a grey-zone of anticipation.

A. Imminent Hostilities as Defined by the WPR

The War Powers Resolution (WPR) provides that hostilities can be a current situation or an imminent situation as

---

[143] S. REP. NO. 102-85, at 46 (1991); *see* Part III.
[144] FIELD MANUAL, *supra* note 10; *see* LAW OF WAR MANUAL, *supra* note 4.
[145] 10 U.S.C. § 395(c)(1)(B)(i) (2018) (" . . . where the armed forces of the United States are involved in hostilities [as that term is used in section 1543 of title 50, United States Code] . . . "); 50 U.S.C. § 1543 (2018).
[146] S. REP. NO. 102-85, at 46 (1991).
[147] *See supra* note 7 and accompanying text.

"clearly indicated by the circumstances. . . "[148] If there is a hostility, then the President must provide notice to Congress pursuant to the procedures of the statute.[149] This has been the topic of intense academic and U.S. intra-branch debate given the broad language used.[150] But, an objective glance at past practice reveals a general consensus of the term's meaning.

---

[148] 50 U.S.C. §§ 1541(a), 1543(a)(1), 1547(c) (2018).

[149] 50 U.S.C. § 1541(a)(2018).

[150] Steven A. Engel, Assistant Attorney General, Office of Legal Counsel, APRIL 2018 AIRSTRIKES AGAINST SYRIAN CHEMICAL-WEAPONS FACILITIES (May 31, 2018) (Slip Opinion) at 1 ("The President's direction was consistent with many others taken by prior Presidents, who have deployed our military forces in limited engagements without seeking the prior authorization of Congress. This deeply rooted historical practice, acknowledged by courts and Congress, reflects the well-established division of war powers under our Constitution. Prior to the Syrian operation, you requested our advice on the President's authority. Before the strikes occurred, we advised that the President could lawfully direct them because he had reasonably determined that the use of force would be in the national interest and that the anticipated hostilities would not rise to the level of a war in the constitutional sense."); Caroline D. Krass, Principle Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice, AUTHORITY TO USE MILITARY FORCE IN LIBYA, MEMORANDUM OPINION FOR THE ATTORNEY GENERAL (April 1, 2011) at 1 (" . . . we concluded that the President had the constitutional authority to direct the use of force in Libya because he could reasonably determine that such use of force was in the national interest. We also advised that prior congressional approval was not constitutionally required to use military force in the limited operations under consideration."); *e.g.* Jack Goldsmith, *Problems with the Obama Administration's War Powers Resolution Theory*, LAWFARE (June 16, 2011), https://www.lawfareblog.com/problems-obama-administrations-war-powers-resolution-theory (last visited, June 13, 2018) ("I do not find the Administration's arguments persuasive . . . [O]ne difficulty in assessing the argument is that the [WPR] does not define 'hostilities.' But common sense suggests that firing missiles from drones that kill people over an extended period of time pursuant to a [U.N].-authorized use of force constitutes 'hostilities.'); *cf.* John Yoo, *War Powers Belong to the President*, American Bar Association (Feb. 2012), http://www.abajournal.com/magazine/article/war_powers_belong_to_the_president (last visited, June 13, 2018) ("President Obama has the Constitution about right. His exercise of war powers rests firmly in the tradition of American foreign policy. Throughout our history, neither presidents nor Congresses have acted under the belief that the Constitution requires a declaration of war before the U.S. can conduct military hostilities abroad.").

The statute itself is concerned with actual *members* of the U.S. military engaging in hostilities, not simply the capability to engage in hostilities. Section 1547(c) of the WPR states:

> "For purposes of [50 U.S.C. §§ 1541 et seq.], the term "introduction of United States Armed Forces" includes the *assignment of members* of such armed forces to command, coordinate, participate in the movement of, or accompany the regular or irregular military forces of any foreign country or government when . . . there exists *an imminent* threat that such forces *will become* engaged, in hostilities" (emphasis added).[151]

The hallmark of this language is that there must be troops assigned to engage in kinetic operations or at least a possibility that they imminently *will be* engaged in kinetic operations.[152] The plain language that a hostility must include armed forces members is supported by the historical backdrop of the WPR.[153] This historical backdrop can be summarized as the legislative branch's concern, particularly in light of operations in Korea and Vietnam involving the prolonged deployment of troops for kinetic operations that resembled war and lacked congressional coordination and approval pursuant to Article I war powers.[154] Due to the use of COPEs as TMAs, the

---

[151] 50 U.S.C. § 1547(c) (2018).

[152] Lorber, *supra* note 7, at 989-991. The author provides insight as to the meaning of § 8(c) of the Act:
As is evident from a textual analysis, an examination of the legislative history, and the broad policy purposes behind the creation of the [A]ct, 'armed forces' refers to U.S. soldiers and members of the armed forces, not weapon systems or capabilities such as offensive cyber weapons . . . given that a core principle of statutory interpretation, *expression unius*, suggests that expression of one thing implies the exclusion of others.

[153] 50 U.S.C. § 1547(c) (2018); Matthew C. Weed, THE WAR POWERS RESOLUTION: CONCEPTS AND PRACTICE, CONGRESSIONAL RESEARCH SERVICE 5 (2017) ("Congressional concern about presidential use of armed forces without congressional authorization intensified after the Korean conflict. During the Vietnam War, Congress searched for a way to assert authority to decide when the United States should become involved in a war or the armed forces be utilized in circumstances that might lead to hostilities.").

[154] 50 U.S.C. § 1541(a) ("It is the purpose of this joint resolution . . . 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

concern, for purposes of this article, is imminent hostilities that will occur as future apparent or acknowledged military operations. Ongoing hostilities would be abundantly clear in a given situation.

In light of language in the WPR, inevitable questions will be raised regarding whether offensive cyber operations conducted as COPEs will themselves require a WPR report. The answer is no. The WPR's legislative history endorses a "members" approach vis-à-vis "imminent hostilities," albeit additional clarification exists in the WPR House Report, providing: "[I]mminent hostilities denote[s] [sic] a situation in which there is a clear potential either for such a state of confrontation or for actual armed conflict."[155] In fact, the executive branch has not hesitated to use this approach, indicating that hostilities can encompass a future serious risk of hostile fire against U.S. armed forces and the exchange of fire between U.S. and opposing units.[156] Furthermore, it is important to note that the executive branch interprets the WPR as inapplicable to independent military operations that are limited in scope, duration, and escalation, and only applicable to prolonged hostilities which resemble a declared war. Discussion of this point is beyond the scope of this article; however, the salient point is that platforms and capabilities are not "members" for purposes of the definition of hostilities.[157]

Perhaps this "boots on the ground" approach is best shown through past administrations' avoidance of WPR notification, as recent air operations in Syria and Libya may not

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."); *see also* U.S. CONST., art. I, § 8.

[155] War Powers Resolution, H.R. 287, at 7 (1973).

[156] Geoffrey Corn, Jimmy Gurelé, Eric Jensen, and Peter Margulies, NATIONAL SECURITY LAW: PRINCIPLES AND POLICY 72-73 (Wolters Kluwer. 2015).

[157] Engel, *supra* note 148. (" . . . the anticipated nature, scope, and duration of the operations were sufficiently limited that they did not amount to war in the constitutional sense and therefore did not require prior congressional approval.").

meet the language of the WPR because no members of the armed forces have been involved in the engagements, only weapons platforms.[158] This approach has worked thus far. Congress has all but failed to hold any administration accountable in the majority of instances when this interpretation is used, with one scholar noting over 160 instances of Presidents committing troops in preparation for combat with minor kinetic engagements, with no Congressional action pursuant to the statute.[159] Adding further complications, the Courts have avoided the issue, in one instance, ruling it constitutes a political question where they lack judicially manageable and discoverable standards for review.[160]

Whatever the case, the point is that 10 U.S.C. § 395 focuses on the *use* of the term "hostilities" in the WPR, not whether a WPR situation exists. But, at-minimum, a "historical gloss"[161] of past practice indicates that offensive cyberspace operations alone do not constitute an introduction of armed forces' members into an area of hostilities, but can assist those

[158] *Id.*

[159] *See e.g.*, Weed, *supra* note 151. The author notes 167 instances where Presidents notify Congress consistent with, but not pursuant to, the WPR.

[160] *Lowry v. Reagan*, 676 F. Supp. 333, 340-41 (1987) ("[I]f the Court were to grant or deny declaratory relief, and decide whether United States Armed Forces . . . are engaged in 'hostilities' or . . . in situations where imminent involvement in hostilities is clearly indicated by the circumstances, the Court would risk 'the potentiality of embarrassment . . . the Court refrains from joining the debate on the question of whether 'hostilities' exist in a region.").

[161] *Youngstown Sheet & Steel Co. v. Sawyer*, 343 U.S. 579, 593-611 (1952) (Frankfurter, concurring). Justice Frankfurter's test emphasis focused on long standing practice between the branches accommodating war powers. This provided meaning and interpretive value to the words of the constitution's bifurcation of war power by providing a "systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by the President" may be treated as a "historical gloss" on executive power. This test contains three essential elements: first, the practice needs to be systematic and long pursued (isolated incidents don't count); second, notice must be given to Congress so as to gauge acquiescence; and lastly, Congress must have not questioned the practice. This process sheds light upon the true meaning of the traceable text given each co-equal branches' obligation to interpret the Constitution and preserve their respective powers. In fact, a length appendix details instances of government property seizure which supplements Justice Frankfurter's opinion. It demonstrates the level of scrutiny required when applying this test in analyzing Presidential actions.

operations that will constitute hostilities given their high probability of occurrence.[162] It would then follow, from the way in which the term "hostilities" is used in the WPR, an offensive cyberspace operation can be conducted to support or "prep" some future military operation (COPE) for a given geographic region. Simultaneously, the support itself will not raise WPR concerns, given it is only a capability that does not constitute an involvement of troops, at least not until members of the armed forces have been exposed to the kinetic engagement. The operation qualifies as a TMA because TMAs encompass hostilities, which are imminent vis-à-vis the terms used in the statute.[163] It also means that, given the level of imminence for an actual hostility for an operation in the geographic region, SMCO oversight would not be raised.[164]As mentioned above, these operations fall within an oversight grey-zone in that are picked up by basic TMA oversight.

B. Examples of Applicability

To demonstrate, the following may be potential results of this analysis:

Example 1: Use of Offensive Cyberspace Operational Preparation of the Environment preceding an imminent hostility. The president orders the start of operations against a hypothetical country who he feels presents a persistent threat to U.S. national security. The country can defend itself against traditional platforms, such as bomber aircraft, drones, and amphibious landings. The mission's objective is to use those platforms to damage the hypothetical country's capability to execute its threats against the U.S. and seize key terrain where those capabilities exist. The U.S. begins to use DoD cyber assets to impact the hypothetical country's defensive capability to facilitate final preparations for an airstrike, bringing the mission into acceptable levels of risk for U.S. armed forces pilots and fair

---

[162] *Id*; *see also* WEED, *supra* note 151.

[163] S. REP. NO. 102-85, at 46 (1991).

[164] 10 U.S.C. § 395(c)(1)(B)(i) (2018) (" . . . where the armed forces of the United States are involved in hostilities [as that term is used in section 1543 of title 50, United States Code] . . . ").

conditions for an amphibious landing on the hypothetical country's soil. Troops are moved off the country's coast in the days beforehand. The operation proceeds, and an announcement is made following the operation's success. This is an appropriate use of COPE. Even if not intended to be apparent or acknowledged, this action would not warrant covert action reporting due to its purposes as a contingency for a larger apparent or acknowledged military operation. The larger operation was ordered by the president, conducted by U.S. armed forces members, and the operation was acknowledged (and most-likely apparent, too). By assisting in setting the conditions for a successful military operation, the COPE preceded the airstrike and amphibious landing, both of which were anticipated to involve U.S. armed forces. Furthermore, due to the high probability and clear indication that the operation was going to involve kinetic engagements between U.S. forces in the region where the COPE occurred, this operation would not be considered a SMCO. The operation is not completely independent from an *imminent hostility* for this geographic region, as the term is used and practiced in accordance with the WPR.

Example 2: Use of Offensive Cyberspace Operational Preparation of the Environment that is not imminent but implemented during ongoing hostilities. Same facts as Example 1, except U.S. armed forces have already been engaged in open and apparent hostilities in the geographic region. This action would not be subject to 10 U.S.C. § 395.[165] Although still covert and a TMA, it is conducted in a geographic region where U.S. armed forces are engaged in ongoing hostilities.

Example 3: Use of Offensive Cyberspace Operational Preparation of the Environment that is apparent and acknowledged, but not clandestine, during ongoing hostilities. Same facts as above, except the U.S. has an intent to acknowledge the operation and conduct it in an apparent manner: the operation is open and overt. There are no efforts made to mask U.S. identity during the operation. This operation is subject to general oversight by the armed forces and will not be subject to

[165] 10 U.S.C. § 395(c)(1)(B)(i) (2018).

any of the aforementioned legal regimes.[166] There is no plausible deniability. The operation occurs in a geographic region where U.S. armed forces are engaged in kinetic operations. It also assists an overall apparent and acknowledged ongoing military operation.

Example 4: Use of Offensive Cyberspace Operational Preparation of the Environment that is expected, but not imminent or ongoing. The President is concerned about the hypothetical country's political instability. Opposition leaders in the hypothetical country have made threats stating that once they take power, they will launch attacks on the U.S. The President orders operational planning for potential military operations should the situation in that country worsen. No decision has been made as to the tactical scheme for the military operation (i.e. assets to be used, maneuvers, etc.). DoD begins using cyber assets to achieve desired effects on the hypothetical country's command and control cyberspace network to aid in its operational planning for this future mission. There is neither an intent to acknowledge the COPE, nor an intent that it be apparent. Although possibly qualifying as a TMA, this action would be subject to 10 U.S.C. § 395 as a SMCO.[167] The expected hostility has not occurred in a geographic region where U.S. armed forces are engaged in ongoing hostilities.[168] Furthermore, the imminent hostilities, although predicted, may be too abstract to justify arguments against reporting to congressional armed services committees.[169]

Example 5: Use of offensive cyberspace operation that is covert. Continuing with the same hypothetical, assume matters have turned for the worst; the political opposition is gaining momentum. The President has ordered the DoD to conduct cyberspace operations against the country's political opposition to affect the opposition's computer network. This operation is intended to be unacknowledged and unapparent. There is no

[166] 10 U.S.C. §§ 394, 484 (2018).
[167] *See* 10 U.S.C. § 395(a), (c) (2018).
[168] 10 U.S.C. § 395(c)(1)(B).
[169] 10 U.S.C. § 395(c)(1)(i); *see also* Part V.A of this article and accompanying text.

future military operation envisioned at the time of the offensive cyber operation. This operation is exempt from 10 U.S.C. § 395 as it is a covert action.[170] Findings and notice will be made to various congressional intelligence committees.[171]

Example 6: Use of Offensive Cyberspace Operational Preparation of the Environment that is clandestine, but not covert. Changing the facts to the above hypothetical, assume that the COPE was intended to be apparent or acknowledged, but conducted in a clandestine manner to ensure that the operation was not discovered by the target country. Notwithstanding the potential foreign policy and foreign affairs issues, this action would be subject to 10 U.S.C. § 395, not the covert action statute.[172] An intent that the operation be acknowledged or apparent exempts this operation from the covert action statute, but not 10 U.S.C. § 395, because hostilities are not present or imminent for U.S. armed forces members.[173]

Example 7: Use of Offensive Cyberspace Operational Preparation of the Environment that primarily collects intelligence. Changing the facts, assume that DoD is merely monitoring and extracting conversations between opposition leaders. No actions have been taken to constitute an offensive cyber operation. This operation is not subject to any of the aforementioned regimes. Although conducted in cyberspace, this is an example of cyber exploitation meant to primarily collect and exploit intelligence. It will be subject to general intelligence

[170] *See id.* §§ 395 (c)(1)(B)(i), (e) ("Nothing in this section shall be construed to provide any new authority or to alter or otherwise affect . . . any requirement under the National Security Act of 1947 [50 U.S.C. 3001 et seq.].").
[171] *Id.* § 395(e). Reporting requirements under the National Security Act of 1947, et. seq. are found in 50 U.S.C. § 3093(b)-(h) (2018).
[172] 50 U.S.C. § 3093(e) (2018) ("'[C]overt action' means an activity or activities . . . where it is intended that the role of the United States Government will not be apparent or acknowledged publicly. . . ."); however, 10 U.S.C. § 395(c)(1)(B)(i) requires hostilities be at-least imminent. *See* Part V.A of this article and accompanying text.
[173] *Id.* and accompanying text.

oversight of the congressional intelligence committees, but not subject to findings and notice procedures.[174]

C. National Defense Authorization Act for Fiscal Year 2019

Section 1632 of the 2019 National Defense Authorization Act affirms the authority of the Secretary of Defense to conduct offensive cyberspace operations as TMAs.[175] This section will have a significant impact on the way that COPEs are conducted, as well as the analysis above. The provision all but quells arguments and debate surrounding whether offensive cyberspace operations as TMAs are "traditional," by explicitly providing that these operations were meant to be TMAs under the covert action statute, regardless of the novel technology.[176] Specifically, and as related to this article, Senate Report 115-262 provides that preparatory actions outside of zones where conflict is occurring are captured within this meaning.[177] The law will, therefore, solidify COPEs as subject to the oversight regimes of the armed services committees, or if certain criteria are met,

---

[174] 50 U.S.C. §§ 3091-3092 et. seq. (2018).

[175] S. REP. NO. 115-262 ("The committee recommends a provision that would affirm the authority of the Secretary of Defense to conduct military activities and operations in cyberspace, including clandestine military activities and operations . . . "); *see also* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, H.R. 5515, 115th Cong. (2018) ("Congress affirms that the Secretary of Defense may conduct military activities or operations in cyberspace, including clandestine military activities or operations in cyberspace . . . ").

[176] S. REP. NO. 115-262, at 330 (2018) ("The committee understands that the authors of the National Security Act used the term 'traditional military activities' to exempt standard military operations and activities from the Act's stringent reporting requirements, designed for the intelligence community's covert action. The authors did not anticipate the cyber domain or the nature of modern cyber conflict and therefore could not establish whether the military's activities in cyberspace qualify as such traditional military activities . . . .[T]he committee believes that clandestine military activities in cyberspace are not just traditional military activities but essential to the military effectiveness of the Armed Forces in modern warfare"); *see* 50 U.S.C. § 3093(e) (2018); *see also* Combe, *supra* note 7, at 541-554.

[177] S. REP. NO. 115-262, at 329 ("The provision would affirm that this authority includes the conduct of military activities or operations in cyberspace short of war and in areas outside of named areas of conflict for the purpose of preparation of the environment . . . ").

those of the intelligence committees' covert action reporting mechanism (discussed, *infra*).

To start, the language of the NDAA provides:

> "[C]ongress affirms that the authority referred to in paragraph (TMAs) includes the conduct of military activities or operations in cyberspace short of war and in areas *outside of named areas of conflict for the purpose of preparation of the environment* . . . "[178]

Notably, the NDAA's language recognizes that cyberspace operations do not need to be conducted within a zone of current conflict. Instead, they can be conducted in areas where the U.S. seeks to prepare a battlespace, i.e. COPEs. These operations will now be dubbed "clandestine activities or operations in cyberspace."[179] A clandestine activity or operation in cyberspace that qualifies as a TMA is defined as a:

> "[m]ilitary activity or operation carried out in cyberspace, or associated with preparatory actions, authorized by the President or Secretary (of Defense) that . . . is marked by, held in, or conducted with secrecy, where the *intent is that the activity or operation will not be apparent or acknowledged publicly;* and is carried out as *part of a military operation plan approved by the President or the Secretary in anticipation of hostilities* or as directed by the President or the Secretary . . . "[180]

If an operation meets this description, the operation will no longer be subject to the covert action reporting and findings mechanisms, but instead will be subject to the new SMCO and quarterly reporting found in 10 U.S.C. § 395 and 10 U.S.C. § 484, respectively.[181] This has another important implication: it

---

[178] *Id.* at 722-23.
[179] *Id.* at 723 ("A clandestine military activity or operation in cyberspace shall be considered a traditional military activity . . . ").
[180] *Id.* at 724. These operations also include the ability to conduct active defense and support military information operations. Such operations are beyond the scope of this article.
[181] 10 U.S.C. § 395 (2018); 10 U.S.C. § 484 (2017). These actions will remain subject to existing AUMFs and the WPR.

focuses oversight away from the overlapping authorities of the intelligence committees by accepting current DoD practice of COPEs, without regard to the labeling or indexing of COPEs for oversight avoidance purposes.[182]

The above definition consists of three core elements: (1) the operation must be approved by the President or Secretary of Defense; (2) there must be an intent for plausible deniability and execution in secret, as defined in earlier portions of this article; and (3) the operation must be carried out as part of an approved operational plan addressing anticipated hostilities against adversaries or emerging threats, or as the President or Secretary of Defense otherwise direct.[183] Depending on the type of operation conducted, other elements may come into play, but for purposes of this article, we are concerned only with this statute's relation to COPEs.

The first element requires that the operation must have National Command Authority approval, which reflects the original TMA legislative language.[184] This element provides the level of internal oversight and decision-making that Congress has wanted since the first TMA language was drafted.[185] Although approval may be more effective at the operational level than the Presidential level, this language resembles past language recognizing authority to carry out covert actions and sensitive military operations, but places the burden of failure on the President's lap.[186]

---

[182] S. REP. NO. 115-262, at 723 (2018); 50 U.S.C. §§ 301-3093 (2018). *See supra* Parts II.B., III, and IV.
[183] S. REP. NO 115-262, at 724 (2018).
[184] *Id.*; *see also* S. REP. NO. 102-85, at 46 (1991).
[185] Chesney (2012), *supra* note 7, at 599.
[186] *See supra* Parts II and IV. *See also* Major Sean B. Zehtab, *Overseeing or Interfering? A Functional Alternative to Congressional Oversight in Intelligence and Operations*, HARV. NAT'L SECURITY J. ONLINE, (June 13, 2018, 10:30 AM), http://harvardnsj.org/2018/06/overseeing-or-interfering-a-functional-alternative-to-congressional-oversight-in-intelligence-and-operations/ (last visited June 22, 2018). The author argues that internal oversight responsibility may be best served at the operational level where combatant commanders exist. Congress involves itself directly in military operations but does not

The second element provides that operations must be conducted with clandestine elements and must be plausibly deniable, thus indicating that operations cannot be open and apparent.[187] To note, "clandestine" in this context has a different meaning than the earlier mention of the term in this article. Here, it is essentially taken to mean a combination of clandestine execution and the traditional meaning of "covert."[188] This may be due to the need to protect means-and-methods for the implementation of national security strategy. Indeed, the report provides that it noted Lieutenant General Paul Nakasone's comments regarding the need to prepare proactively in adversary cyberspace networks.[189] The Senate report concludes, based upon these concerns, that the U.S. military must have the ability to clandestinely operate and access relevant enemy systems and networks.[190]

The third element provides that there must be an operational plan in place that is approved by the President and addresses predicted hostilities.[191] Again, this ensures that responsibility for these operations is located at the appropriate level, given the geopolitical and policy implications. Although the level of detail of the plan is not described in the statute's language, this requirement rids the old TMA analysis of abstraction for anticipated hostilities, as argued above under the current regime.[192] The old argument would follow that the

provide the resources to forces actually carrying out the mission to remain compliant with the complex oversight regime. Instead, Congress focuses its efforts at the highest level of command.

[187] S. REP. NO. 115-262, at 72.

[188] *Supra* Part II.A; *see also* S. REP. NO. 115-262, at 723.

[189] *Id.* at 330 ("The committee asserts that persistent cyber operations in adversary networks, or 'red space,' are critical for the development of military and deterrence targets. As Lieutenant General Paul Nakasone stated on February 27, 2018, in his response to the committee's advance policy questions for his nomination to be the Commander, U.S. Cyber Command and the Director of the National Security Agency, 'to be operationally effective in cyberspace, U.S. forces must have the ability to conduct a range of preparatory activities, which may include gaining clandestine access to operationally relevant cyber systems or networks.'").

[190] *Id.*

[191] *Id.* at 724.

[192] *See* Part V.

existence of an operational plan indicates a level of anticipated hostilities rather than mere speculation that they will occur. The plan would objectively show oversight authorities that substantial steps taken by the President prove the existence of the anticipated hostility. Now an operational plan is mandated. It appears to justify that a hostility is imminent for purposes of avoiding SMCO. There must be a substantial step taken to draw a line between those hostilities, which are merely anticipated rather than imminent.[193] An operation without a plan authorized by the President is still considered a TMA but may not contain the caveats of a planned operation.

What can be drawn from this language is that the beginning of any analysis for a geographically independent offensive cyberspace operation is no longer a query of the covert action statute and TMA exception, but whether the operation must be reported under the SMCO regime or only the quarterly briefing, cited *supra*. This is because these operations are categorically exempt from covert action language, and instead are considered TMAs (COPEs for purposes in this article).[194]

Although these operations are subject to SMCOs and quarterly reports, and no longer the covert action statute, the new language does not take away the possibility that these operations will avoid the SMCO statute's 48-hour rule.[195] A determination must still be made whether the operation is wholly independent of a hostility (or "conflict" as used in the 2019 NDAA) or part of one that is ongoing or imminent.[196] The analysis in Part V does not change because SMCOs require current hostilities, as provided in the War Powers Resolution.[197] If the operation is wholly independent of any imminent hostility

---

[193] *See generally*, Lieutenant Commander Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar"*, 22 FLA. J. INT'L L. 333, 345-56 (2010). The author provides historical examples of substantial steps taken to justify the "anticipation" such as prepositioning of traditional assets, then draws the comparison to cyberspace with prepositioning of cyber payloads.
[194] S. REP. NO. 115-262, at 723.
[195] 10 U.S.C. § 395 (2018); Part V.
[196] *Id.*
[197] *Id.*

and is anticipated as shown through operational plans, it will be subject to both reporting regimes (such as those merely directed by the President or Secretary of Defense). If steps have been taken to cross the threshold of anticipation into that of imminence, it will only be reported in the quarterly report.

VI. CONCLUSION

The task of reconciling a new development in law with those of the old necessitates a resolution of the legal impact it will have on its predecessors. The solution must consider what has been created, its place amongst the current regime, and what is now established.[198] Objectively, it would be a mistake to assume that 10 U.S.C. § 395 classifies all COPEs as TMAs not subject to granular reporting for *all* independent actions outside of a geographic region where troops are engaged in ongoing hostilities. What appears to be true, however, is that under this new regime there must be at least some indication of a realistically planned kinetic military action, as opposed to one which simply exists in the abstract (notwithstanding a possible new requirement by the 2019 NDAA). 10 U.S.C. § 395 appears to tighten the temporal and geographic nexus for COPEs that are indexed as TMAs with regard to anticipated hostilities by now requiring that, at minimum, there be a level of imminence within a geographic region of occurrence. If this can be shown through operational plans and orders, coupled with steps taken to objectively indicate a realistic possibility of hostilities, COPEs may continue to be subject to general oversight, as opposed to the more stringent reporting mechanisms discussed throughout this article.

[198] William Baude and Stephen E. Sachs, *The Law of Interpretation*, 130 HARV. L. REV. 1079, 1083 (2017).