INTERNATIONAL LAW STUDIES

PUBLISHED SINCE 1895

U.S. NAVAL WAR COLLEGE

Computer Network Operations and U.S. Domestic Law: An Overview

Robert M. Chesney

89 INT'L L. STUD. 218 (2013)

Volume 89 2013

Computer Network Operations and U.S. Domestic Law: An Overview

Robert M. Chesney[*]

I. INTRODUCTION

Computer network operations (CNOs) famously give rise to a number of international law complications, and scholars have duly taken note.[1] But

* Charles I. Francis Professor in Law, University of Texas School of Law.

1. This was, of course, the primary subject of the conference of which this article was a part. *See* U.S. Naval War College International Law Department, 2012 ILD Conference: "Cyber War and International Law," http://www.usnwc.edu/ILDJune2012. It was also the subject of the International Law Department's 1999 conference, "Computer Network Attack and International Law." The papers resulting from that conference may be found in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies). For a sampling of the considerable literature focused on the international law questions raised by CNOs, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817 (2012); Hannah Lobel, *Note: Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict,* 47 TEXAS INTERNATIONAL LAW JOURNAL 617 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 VILLANOVA LAW REVIEW 569 (2011); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533 (2010); Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 63 (2010). *See also* TALLINN MANUAL ON

CNOs also raise important questions under the heading of U.S. domestic law, particularly when the government does not intend for its sponsoring role to be apparent or acknowledged. Those domestic issues have received comparatively little attention.[2]

This article introduces readers to four of the most important domestic law questions raised by CNOs, drawing on my prior work exploring the disruptive impact of organizational and technological change on the legal architecture of national security activities.[3] First, must Congress be notified of a given CNO and, if so, which committee should receive that notice? Second, must the CNO in question be authorized by the President himself, or can authority be moved down the chain to other officials—or perhaps even automated? Third, what is the affirmative source of domestic law authority for the executive branch to conduct various types of CNO? Fourth, and finally, does categorizing a CNO as covert action subject to Title 50 of the U.S. Code (U.S.C) carry with it a green light (from a domestic law perspective) to violate international law?

II. MUST CNOS BE REPORTED TO CONGRESS?

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.

This general topic is familiar to American national security law practitioners from the context of covert action. Pursuant to § 503 of the Nation-

---

THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

2. Notable exceptions that address domestic issues at least in part include Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations,* 111 MICHIGAN LAW REVIEW 423 (2012); Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEORGE WASHINGTON LAW REVIEW 1162 (2011); Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARVARD NATIONAL SECURITY JOURNAL 591 (2011); Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar,"* 22 FLORIDA JOURNAL OF INTERNATIONAL LAW 333 (2010).

3. *See* Robert M. Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 539 (2012).

al Security Act, the executive branch must provide notification of a "covert action" to the Intelligence Committees (though notification can be limited in "extraordinary circumstances" to the "Gang of Eight"—i.e., the chairs and ranking members of both committees, as well as the Speaker and Minority Leader in the House and the Majority and Minority Leaders in the Senate).[4] "Covert action," in turn, is defined by statute to mean "an activity . . . of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the . . . government will not be apparent or acknowledged publicly . . . ."[5]

So far so good. It is easy to understand how a CNO conducted for purposes of sabotage, for example, implicates that definition at first blush. But the statute goes on to carve out a series of exceptions to the covert action definition,[6] two of which make it relatively difficult to determine—particularly in advance—whether a given CNO triggers the covert action oversight framework.

First, an otherwise-qualifying activity does not count as "covert action" if its "primary purpose . . . is to acquire intelligence . . . ."[7] A CNO certainly might be designed primarily to acquire intelligence, whether through keystroke logging, network mapping, microphone or camera control, or data copying.[8] But this turns out to be irrelevant insofar as congressional notification is concerned, because the National Security Act separately provides that significant intelligence activities—including activities to collect intelligence—also must be reported to the Intelligence Committees.[9] Categorizing a CNO as intelligence-gathering rather than covert action thus does nothing to alter the obligation to keep Congress informed.

The second relevant exception to the definition of covert action is different. It encompasses "traditional . . . military activities" (often referred to as TMA) and "routine support" thereto.[10] When it applies the executive branch has no obligation to keep the Intelligence Committees informed of the activities in question, period.

---

4. 50 U.S.C. § 413b(b), (c) (2006).

5. *Id.*, § 413(e).

6. *Id.*, § 413(e)(1–4).

7. *Id.*, § 413(e)(1).

8. *See, e.g.,* Kim Zetter, *State-Sponsored Malware "Flame" Has Smaller, More Devious Cousin*, WIRED (Oct. 15, 2012, 8:00 AM), http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/

9. 50 U.S.C. §§ 413, 413a (2006).

10. *Id.*, § 413(e)(2).

Consider first the scope of the TMA exception. The text of the statute does not define TMA. This naturally tempts some to assume that the key to identifying activity as TMA involves some form of comparison to past practices particularly associated with the military. The word "traditional" in TMA, after all, suggests precisely this comparison. If that were indeed the correct reading, substantial debates would then arise in light of the relative novelty of CNOs. In order to categorize a CNO as TMA, one would first have to establish that the TMA standard could be satisfied via analogy rather than requiring a literal precedent showing the military previously engaged in that exact type of operation. If that bridge were crossed, moreover, one would then have to show that the CNO in question does in fact track the relevant contours of some past, non-cyber military operations. The history-based interpretation of TMA, in short, invites no small amount of disagreement and instability. But it is far from clear that the history-based interpretation of TMA is correct in the first place.

The legislative history of the TMA exception is long and dense, and I have set it forth in its full complexity elsewhere.[11] For present purposes, it suffices to observe that Congress and the administration of George H.W. Bush negotiated this question extensively, and ultimately compromised by adopting a relatively objective definition of TMA.[12] Two conditions had to be met, no more and no less. First, the activity had to be commanded and executed by military personnel. Second, the activity had to take place in a context in which *overt* hostilities either were under way already or at least were "anticipated" in the specific sense that the National Command Authorities had authorized "operational planning for hostilities."[13] Historical comparisons simply did not enter into the picture, on this view.

This understanding—*if* accepted by all sides engaged in an internal debate over the applicability of the TMA exception in a given case—should prove relatively easy to map onto CNOs in some contexts. Most obviously, any CNO linked to overt combat operations, such as those currently under way in Afghanistan, should qualify without controversy (so long as commanded and executed by military personnel). Similarly, an operation like Stuxnet—involving a potential adversary regarding which it is quite possi-

11. *See* Chesney, *supra* note 3, at 592–601. *See also* Walker, *supra* note 2.

12. *See* Walker, *supra* note 2, at 340 (citing S. REP. NO. 102-85, at 46 (1991); H.R. CONF. REP. 102-166 (1991)).

13. S. REP. NO. 102-85, at 46 (1991).

ble if not probable that operational planning has been authorized—likewise would qualify so long as commanded and executed by military personnel.[14]

Why then might there still be controversy with respect to TMA's scope? First, it is not obvious that the objective, negotiated definition just discussed is, in fact, widely appreciated within the government, let alone widely accepted as controlling. It is memorialized only in the legislative history rather than the actual text of the statute, after all, and it does not follow intuitively from the words "*traditional* military activity." Second, even if one accepts the objective test, there remains significant room for disagreement regarding its actual application, particularly thanks to ongoing uncertainty over the organizational, geographic and temporal scope of hostilities relating to al Qaeda and the conflict once called the "war on terror."

And what of "routine support" to TMA? This too was the subject of considerable attention during the drafting of the covert action definition.[15] Rather than adopt specific criteria to explain the boundaries of the routine support concept, Congress in the legislative history provided an illustrative set of examples. Unacknowledged logistical support for a potential military operation would count, for example, whereas recruiting foreign personnel or engaging in propaganda would not. The difference, according to the legislative history, was that the latter were riskier activities for the United States, hence less appropriate for exemption from the oversight system. That risk-oriented distinction can be brought to bear on the question whether a given CNO constitutes routine support to TMA, but one should expect there to be many circumstances in which reasonable minds can disagree as to the outcome; the nature of this criterion is simply too subjective, whether we are speaking of CNOs or non-cyber activities.

In any event, let us assume now that a given CNO qualifies as TMA or routine support thereto. Might there still be an obligation to report it to Congress?

---

14. This helps us make sense of what David Sanger reports with respect to Stuxnet:

> At the insistence of Defense Secretary Robert Gates, the program had been shifted over from military command to the intelligence community. That meant that President Obama had to review and renew a set of presidential findings that would allow the United States to attack the nuclear infrastructure of a country with which we were not at war.

DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 200–201 (2012). A presidential "finding," as I explain below in Part II, becomes necessary only upon a determination that the activity is a covert action rather than TMA.

15. *See* S. REP. NO. 101-358, at 54 (1990).

On one hand, 10 U.S.C. § 119 does specify that new special access programs may not be initiated by the Department of Defense without notification to the Armed Services Committees.[16] This might encompass some CNOs. But it would not necessarily encompass all of them, and in any event would not require the sort of detailed, high-granularity exchange of information that can arise with covert action oversight. Of course, relatively detailed reporting *might* occur even without an explicit statutory obligation; the Armed Services Committees and their staffs obviously have significant leverage, and as a practical matter can demand no small amount of transparency if the leadership so desires. At 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.

III. MUST CNOS BE APPROVED BY THE PRESIDENT?

Whether a given CNO constitutes covert action has implications beyond notification to Congress. The National Security Act not only requires reporting of covert action to the Intelligence Committees, but also specifies that such activity must be authorized in a written "finding" signed by the President. This requirement of a presidential finding serves to constrain the executive branch in at least a couple of ways. First, and most obviously, it precludes the President from later denying knowledge of what might turn out to be a controversial action, thus giving rise to top-down pressure to screen out risky proposals (for better or worse). Second, and relatedly, the process of generating a presidential finding generally involves input from multiple departments, some of whom may have distinct or competing equities at stake and hence incentive to argue for modification or rejection of the proposal.

Categorizing a CNO as covert action automatically brings these constraints to bear. But as I explained in Part I there are circumstances in which a CNO might more accurately be characterized as either TMA or intelligence collection. What then?

If a CNO constitutes TMA, the question whether a statute requires approval from a particular official becomes complicated. At first blush, there appears to be no such obligation. And that is indeed the end of the analysis for those who reject the negotiated definition of TMA (described above in

16. 10 U.S.C. § 119 (2006).

Part I). Those who accept the negotiated definition, however, must go on to ask one further question. Recall that the negotiated definition of TMA distinguishes between activities conducted in the context of ongoing hostilities and those conducted in relation to anticipated hostilities for which operational planning has been authorized. Under the ongoing-hostilities track, there is no requirement that a particular official approve the activity in question in order for it to qualify as TMA. But under the anticipated-hostilities track, the answer is different. The negotiated definition specifies that the activity must be approved by the National Command Authorities—i.e., the President or Secretary of Defense—in order for it to qualify as TMA in such circumstances.[17]

What if the CNO in question instead is best understood as intelligence collection rather than covert action or TMA? I noted in Part I that classification of a CNO as collection did not alter the obligation to report the activity to the Intelligence Committees. The intelligence-collection/covert action distinction does matter, in contrast, with respect to the question of statutorily required authorization. Whereas a presidential finding is required for covert action, there is no parallel or comparable statutory requirement for intelligence-collection operations.

Unfortunately, it is not necessarily easy to apply the intelligence-collection/covert action distinction, particularly in the CNO setting. The code in question may involve a complex suite of tools including not just capacities for collection, but also capacities to disrupt or modify the operation of an infiltrated system or server (as appears to have been the case with the so-called Stuxnet CNO directed at Iran).[18] The "primary purpose" criterion built into the statutory language anticipates such dual-use problems in the abstract, calling for what amounts to a center-of-gravity test. That inquiry is both subjective and dependent upon timing, however. What might seem to be the code's primary purpose might appear to be collection at one point in time, and disruption at some later point (e.g., after the previously latent destructive capacity of the code has been employed). The National Security Act, alas, does not provide guidance regarding which moment is the correct one on which to focus or whether the inquiry should be conducted repeatedly over time.

Of course, a statute is not the only means by which a requirement of high-level approval for CNOs could be imposed. The President himself

17. *See supra* note 13 and accompanying text.

18. *See* SANGER, *supra* note 14, at 190–206.

can issue such a mandate, after all, and it does appear from the public record that something along these lines has occurred. A series of media accounts in recent years tell the tale of long-running interagency disputes as the Pentagon attempts to craft rules of engagement determining when CNOs might be conducted in contexts that could have adverse effects on systems physically located outside the United States, with at least some circumstances marked as off-limits without presidential approval.[19]

IV. MUST CNOS BE SUPPORTED BY CONGRESSIONAL AUTHORIZATION?

CNOs come in many shapes and sizes, some of which are uninteresting from a separation-of-powers perspective. Those that are best analogized to intelligence gathering, for example, should be relatively easy to explain with reference to the same combination of Article II constitutional authorities and statutes that justify such activity in non-cyber settings.[20] Where a CNO instead constitutes TMA or covert action, however, difficult (or at least more interesting) questions can arise.

As a threshold matter, it is worth noting that separation-of-powers concerns drop out to the extent that a given CNO falls within the scope of a statutory authorization for use of military force, such as the still-operative Authorization for the Use of Military Force (AUMF) enacted after 9/11.[21] That AUMF famously provides that the President may use "all necessary and appropriate force" against those entities or individuals he determines were responsible for the 9/11 attacks, as well as entities or individuals harboring them. In some instances involving CNOs, it will be fairly obvious that the AUMF applies. If the Afghan Taliban have a recruiting website hosted on a server in Afghanistan, for example, a U.S. Cyber Command

19. *See* Ellen Nakashima, *Pentagon Seeks More Powers for Cyberdefense*, WASHINGTON POST, Aug. 10, 2012, at A1; Lolita Baldor, *Pentagon Still Grappling with Rules of Cyberwar*, ASSOCIATED PRESS, July 25, 2012, *available at* http://www.foxnews.com/us/2012/07/25/pentagon-still-grappling-with-rules-cyberwar/; Ellen Nakashima, *A Cyberspy Is Halted, but Not a Debate,* WASHINGTON POST, Dec. 9, 2011, at A1; ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S SECRET CAMPAIGN AGAINST AL QAEDA 135–36, 145–46 (2011).

20. *See* Williams, *supra* note 2, at 1167 ("Authority for foreign intelligence collection by the United States Government is grounded in the 'firm foundation' of the Constitution, the National Security Act of 1947 . . . and the Central Intelligence Act of 1949, as well as the many congressional appropriations for intelligence activities.").

21. *See* Pub. L. No. 107-40, 115 Stat. 224 (2001) (Sept. 18, 2001). For a detailed and insightful discussion of this topic, see Brecher, *supra* note 2.

operation to disrupt that website rather plainly would fall within the AUMF's scope. If that server is instead located in Dubai or Germany, however, and if the organization in question is not al Qaeda or the Afghan Taliban but instead some meaningfully-distinct group, things begin to look less clear. Prompted by controversy surrounding detention and drone strikes, there has for many years been a debate about the AUMF's precise boundaries in terms of its geographic and organizational scope, and that debate is growing more serious over time as the center of gravity for AUMF-related operations moves away from Afghanistan, the Afghan Taliban, and the core al Qaeda leadership.[22] CNOs may have implicated these questions in the past; they certainly will do so in the future.

If a given CNO does *not* plausibly fall within the scope of the AUMF, what then? Many non-AUMF CNOs are best categorized as intelligence-collection operations, as noted above, and those typically do not raise significant separation-of-powers concerns. Other non-AUMF CNOs instead constitute covert action or TMA, yet should not be controversial from a separation-of-powers perspective either, because they may be supported by other forms of statutory authorization or by plausible claims that they are within the scope of the President's Article II authorities. A CNO conducted by the Central Intelligence Agency (CIA) as covert action, for example, may rest on the same statutory foundation as any other covert action conducted by the agency: i.e., the National Security Act's "fifth function" as fleshed out over time by executive branch practice, congressional acquiescence in that practice and subsequently enacted oversight legislation.[23] And at least some instances of non-AUMF CNOs constituting either covert action or TMA (particularly those that are distant in their nature or effects from the use of kinetic force) might be relatively easy to justify as exercises of the constitutional authority of the President to conduct foreign affairs or to command the armed forces.[24]

Is the latter still true for a CNO with significant kinetic effects, such as Stuxnet?[25] In 2011, the Obama administration contended that its sustained,

22. *See* Robert M. Chesney, *Beyond the Battlefield, Beyond al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, MICHIGAN LAW REVIEW (forthcoming 2013).

23. *See, e.g.,* William C. Banks & Peter Raven-Hansen, *Targeted Killing and Assassination: The U.S. Legal Framework*, 37 UNIVERSITY OF RICHMOND LAW REVIEW 667, 698 (2003).

24. *Cf.* Robert F. Turner, *Coercive Court Action and the Law,* 20 YALE JOURNAL OF INTERNATIONAL LAW 427, 442–45 (1995) (reviewing W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW (1992)).

25. *See* SANGER, *supra* note 14.

overt use of airpower in Libya (including both comprehensive logistical support to combat sorties carried out by NATO and other allies, and periodic airstrikes using U.S. manned and unmanned aircraft) fell within the President's constitutional authority to act in foreign affairs in pursuit of significant national interests, and that this did not infringe congressional prerogatives over the resort to war in light of the limited nature of the force involved, the limited purposes for which it was being used, and the fact that the situation did not entail a significant risk of harm to U.S. personnel.[26] Few if any CNOs would run afoul of that narrow understanding of the congressional role. That said, the Obama administration's theory of authority vis-à-vis Libya has been met with sharp criticism, and reliance exclusively upon it might be unnecessarily risky.[27] If the circumstances warrant the argument,[28] it would be wise instead (or at least in addition) to invoke the President's constitutional duty to use force in self-defense, a duty which if otherwise implicated can surely encompass CNOs.[29]

---

26. *See* Office of Legal Counsel, *Authority to Use Force in Libya*, 35 Op. O.L.C. (Apr. 1, 2011), *available at* http://www.justice.gov/olc/2011/authority-military-use-in-libya.pdf.

27. *See, e.g.,* Michael D. Ramsey, *Meet the New Boss: Continuity in Presidential War Powers?*, 35 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 863, 864 (2012).

28. The precise boundaries of self-defense authority are famously difficult to define. Much of the literature on this subject arises in the international law setting. *See, e.g.,* Matthew C. Waxman, *The Use of Force Against States That Might Have Weapons of Mass Destruction*, 31 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1 (2009). To at least some extent, however, the insights of the international law debate can be mapped onto the parallel separation-of-powers questions associated with the President's self-defense authority. In practical terms relating to CNOs, the hardest questions may arise when the government acts in an anticipatory rather than reactive setting. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 932–33 (1999). *See also* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARVARD JOURNAL OF LAW & TECHNOLOGY 415, 526–28 (2012); David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 90 (2010).

29. David Sanger's account of the internal debates of the Obama administration in relation to the use of force in Libya in 2011 raises an interesting question. According to his account, U.S. officials at one point considered conducting a CNO that might disable Libya's air defense network, prior to overt military intervention. *See* SANGER, *supra* note 14, at 344. The proposal came to naught in the face of technical difficulties, but along the way it apparently generated a legal dispute "about whether the President had the authority . . . to order a cyberattack as part of a broader military operation without first consulting Congress." *Id.* It is unclear how resort to a CNO could possibly have raised different separation-of-powers concerns than the overt, kinetic measures the Obama administration was contemplating, let alone concerns with more bite. It may be that the actual concern in this instance had more to do with fear of exposure of U.S. CNO capacities that might follow

Against this backdrop, one final question arises: For the subset of cases in which congressional authorization at least arguably is necessary, has Congress already provided such authorization separate and apart from the AUMF? This question draws our attention to § 954 of the National Defense Authorization Act for Fiscal Year 2012. That statute provides as follows:

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

The interesting question here is whether § 954 should be read to authorize CNOs in circumstances beyond what would be covered in any event either by the AUMF or by a plausible claim of inherent presidential authority, or whether instead § 954 merely confirms existing authority for clarity's sake (and perhaps also to dispel doubt that such existing authority requires compliance with the War Powers Resolution and various other regulatory regimes that would govern Department of Defense kinetic operations). Section 954 is clearly superfluous as an authorizing mechanism insofar as it contemplates CNOs in circumstances genuinely involving national self-defense. Whether the same can be said for the statute's explicit reference to "offensive" CNOs undertaken in the defense of "Allies and interests," however, is much less clear.

On its face, this language might be taken as a standing authorization to engage in CNOs for a rather wide range of purposes beyond those for which it is quite apparent authority already exists. But did Congress actually intend that result? There is reason to believe it did not, though the matter is far from conclusive.

The original version of this section—§ 962 in the House bill—simply stated that the military had authority to engage in CNOs on a clandestine basis when acting under color of the AUMF or "to defend against a cyber

---

from disclosure to Congress (under the War Powers Resolution (WPR)) that the United States had engaged in such an operation. Or it may simply be that participants in this debate took the view that a CNO of this kind would amount to the introduction of U.S. forces into hostilities, triggering the consultation language in section 3 of the WPR.

attack against an asset of the Department of Defense."[30] That language would have done little work other than helping to clarify the TMA/covert action distinction as applied to CNOs. Later, during the conference reconciliation process, that text was replaced by the language that became § 954—language that does not obviously speak to the TMA/covert action question. Despite this, the explanation for § 954 published by the conference committee focused on precisely that question:

> The conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes *traditional military activities* in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities.[31]

Of course, the conference committee report also proceeded to address a separate point:

> The conferees also recognize that in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged. The conferees stress that, as with any use of force, the War Powers Resolution may apply.[32]

Seen in this light, § 954's reference to "offensive" CNOs might best be understood to use "offensive" in the tactical sense of taking the initiative to attack the enemy in a particular instance, as distinct from the larger constitutional sense in which one might ask whether the U.S. government is initiating hostilities or instead acting overall in a defensive capacity. From this perspective, it is possible to undertake offensive operations while still under a larger defense rubric, and if that is indeed what § 954 is referring to then there is much less basis for construing the statute as a blank check to conduct CNOs in otherwise inappropriate circumstances.

---

30. National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Cong. § 962 (2011).

31. Explanation of Funding Summary 146 (emphasis added), http://democrats.rules.house.gov/112/text/112_hr1540mgrs_txt.pdf(last visited Nov. 10, 2012).

32. *Id.*

V. MUST CNOS COMPLY WITH INTERNATIONAL LAW?

CNOs raise an array of international law issues, including questions of compliance with the law of armed conflict and international law protection for the sovereignty of States. Strictly speaking, such questions are beyond the scope of this article, as I am focused here exclusively on questions of domestic law.[33] There is, however, an important domestic law question lurking in the background when the subject of CNOs and international law arises: Does the statutory authority to conduct covert action under Title 50 entail standing, domestic law authorization for the executive branch to place the United States in violation of otherwise-applicable international law?

I previously addressed this question in some detail in the midst of a much-longer exploration of the so-called Title 10/Title 50 debate.[34] Nothing in Title 50, I observed then, explicitly authorized operations in violation of international law, nor did the legislative history of the covert action provisions of Title 50 suggest that Congress intended to confer a standing authorization to act contrary to international law rules so long as the government acted covertly.[35] There is, though, an additional argument I did not previously address.

The argument arises out of a conspicuous omission in § 503 of the National Security Act (50 U.S.C. § 413b(a)). Section 503 specifies that a presidential finding authorizing covert action may not call for conduct that would violate the Constitution or any federal statute. It says nothing of the kind, in contrast, about compliance with international law.[36] Did Congress intend thereby to authorize covert action in violation of international law, albeit without saying so explicitly?

It is possible that the executive branch reads Title 50 in this manner, yet it is far from certain that it does so. The most recent and detailed glimpse into the CIA's own perspective on its legal compliance obligations is a speech delivered at Harvard Law School in April 2012 by the CIA's General Counsel, Stephen W. Preston. In it, Preston provided an overview of how his office works through questions of domestic and international

33. *See, e.g.,* TALLINN MANUAL, *supra* note 1.
34. *See* Chesney, *supra* note 3, at 617–28.
35. *See id.*
36. *See* 50 U.S.C. § 413b(a)(5) (2006).

law compliance.[37] With respect to domestic law, Preston was clear about the CIA's compliance obligations: "[A]ll steps taken must comply with applicable prohibitions and limitations in the U.S. Constitution, federal statutes, executive orders and other presidential directives, and Agency regulations."[38] He separately observed that "international law principles may be applicable as well," later elaborating that if the CIA were to conduct operations involving the use of lethal force it "would implement its authorities in a manner consistent with the four basic principles in the law of armed conflict governing the use of force . . . ."[39] Some observers construed this language as indirect acknowledgment that the CIA does not actually think itself bound by international law, even if it does choose to comply with "principles" derived therefrom.[40] Notably, in this regard, the speech did include a pointed quotation of § 503, describing it as a "crucial provision" that "would be strictly applied in carrying out our hypothetical program."[41]

It is difficult to say whether this was a veiled acknowledgment that § 503 is understood within the CIA as permitting the President to direct the CIA to engage in conduct that might violate international law, or if instead it merely reflected a disposition to speak more directly about domestic law as the primary focus of legal review in such cases. The question does seem to matter in practice for CNOs, though, in light of the genuine prospect of undesired third-country (or at least third-party) effects. As one anonymous U.S. government official put the point recently: "Operations in the cyberworld can't be likened to Yorktown, Iwo Jima or the Inchon landing . . . . Defining the battlefield too broadly could lead to undesired consequences, so you have to manage the potential risks. Getting to the enemy could mean touching friends along the way.[42]"

More specifically, "getting to the enemy" with a CNO could mean disrupting the operation of a system or server that is physically located in the territory of a State that is not an enemy and that might not have consented

37. Stephen W. Preston, *CIA and the Rule of Law*, 6 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 1 (2012).

38. *Id.* at 3.

39. *Id.* at 3, 7.

40. *See, e.g.,* Deborah Pearlstein, *CIA General Counsel Speech on Hypothetical Uses of Force*, OPINIO JURIS (Apr. 11, 2012), http://opiniojuris.org/2012/04/11/cia-general-counsel-speech-on-hypothetical-uses-of-force/.

41. Preston, *supra* note 37, at 6.

42. Ellen Nakashima, *Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield*, WASHINGTON POST (Nov. 6, 2010, 12:41 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/ar2010110507304.html.

to the intrusion, with damaging collateral consequences for any number of entities around the world who happen also to rely on those systems or servers. In addition to posing a policy dilemma, this fact pattern also raises international law questions—and hence collateral questions regarding international law compliance obligations when acting under the covert action rubric. The *Washington Post* reports that a dispute arising out of such concerns was put to the Justice Department's Office of Legal Counsel in 2010, resulting in a draft opinion to the effect that "[o]perations outside a war zone would require the permission of countries whose servers or networks might be implicated."[43] It was not clear, alas, whether the draft opinion specifically addressed the covert action question described above.[44]

VI. CONCLUSION

From a domestic law perspective, CNOs present a host of interesting and difficult questions. By and large they are the same questions that surround other forms of government activity in which the government's role might not be apparent or acknowledged. This overlap does not mean there are clear answers to the questions, however. In important respects, the law remains underdeveloped, and in any event the particular characteristics of CNOs at times may make these frameworks particularly difficult to apply.

43. *See id.*

44. It is important to bear in mind that there may be *other* reasons why the CIA, for example, might enjoy greater discretion than the military to conduct certain operations in certain locations. Most obviously, this will be the case where the military acts pursuant to an execute order that contains relatively strict constraints relating to which activities can be conducted in which locations, while the CIA acts pursuant to a covert action finding with broader parameters.