University of Virginia School of Law

Public Law and Legal Theory Research Paper Series 2013-10

The Geography of Cyber Conflict: Through a Glass Darkly

Ashley Deeks

University of Virginia School of Law

March 2013

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1901
U.S. NAVAL WAR COLLEGE

The Geography of Cyber Conflict: Through a Glass Darkly

Ashley Deeks

89 INT'L L. STUD. 1 (2013)

Volume 89 2013

The Geography of Cyber Conflict: Through a Glass Darkly

Ashley Deeks[*]

I. INTRODUCTION

Imagine an Israeli Air Force jet is shot down in international airspace just outside Turkish airspace. Imagine further that the Israel Defense Forces (IDF) and Israeli intelligence services quickly ascertain with a high level of confidence that a Hezbollah cell located in Turkey was responsible for the shoot-down. Israel now confronts a difficult question: having suffered an armed attack, may it use force in self-defense against a non-state actor in the territory of a state with which it is not in an armed conflict and that was not the author of the attack?

In previous work, I have argued that Israel may only take action in Turkish territory against Hezbollah if it has Turkish consent or if it determines that Turkey is unwilling or unable to suppress the threat posed by Hezbollah.[1] This "unwilling or unable" test, which has analogical roots in

* Associate Professor of Law, University of Virginia School of Law.

1. *See generally* Ashley Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012).

the law of neutrality,[2] serves as an attempt to balance the security of the State that suffered the attack (the "victim State") against the sovereignty of the State from which the non-State actor launched the attack (the "territorial State"). The test also reflects the international community's interest in reducing to the lowest level feasible inter-State conflict (and State uses of force in self-defense).

Imagine now that the IDF learns that its air force's command and control center is being severely compromised electronically and has begun to send faulty coordinates to all of the IDF's military aircraft, including those currently airborne. As a result of the cyber attack,[3] the IDF loses communications with two of its jets, which crash into the Mediterranean Sea. Israel has a high level of confidence that several servers in Turkey are the source of the ongoing attack; additionally, the offending code behind the attack has Hezbollah's digital fingerprints on it and Israel has intelligence that Hezbollah has been trying for several years to conduct just such an attack. Assuming that Israel has the technological capacity to disable the Turkish servers currently routing the attack and believes that such an action is the only way to stop this attack, may Israel disable those Turkish servers (using cyber or kinetic tools)? What, if anything, must it do first?

This article argues that the "unwilling or unable" test applies to this scenario as well, although the issues facing Israel and Turkey in the two scenarios are different in important ways. Other scholars have suggested that the "unwilling or unable" test is relevant in the cyber context,[4] but no

---

2. J.M. SPAIGHT, WAR RIGHTS ON LAND 482 (1911) ("[W]here the neutral cannot or will not enforce its rights, then the belligerent is fully entitled to prevent the violation permitted by the neutral redounding to his disadvantage.").

3. This paper uses the phrase "cyber attacks" generically to refer to acts that "alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks," TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (WILLIAM OWENS, KENNETH DAM, & HERBERT LIN, EDS., 2009) [hereinafter OWENS ET AL.]. A particular cyber attack may or may not constitute a use of force or armed attack, as those terms are used in the *jus ad bellum* sense.

4. *See* Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1050 (2007) ("International law contemplates that the [State injured by information operations] would notify the State from whose territory it believes the IO originated and request that State put a stop to it. The requested State is expected to comply with such requests . . . . Only if the requested State is unable or unwilling to stop the IO can the aggrieved State take counter-measures (or perhaps exercise a right of self-defense against the requested State . . . ."); George Walker, *Information Warfare and Neutrality*, 33 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 1079, 1199 (2000)

scholar has analyzed how a State actually should or would apply that test, how the test's application will differ in the cyber and non-cyber contexts and what that divergence teaches us about conflict in the cyber realm. This paper addresses those three issues, focusing on situations in which the cyber activity rises to the level of a cyber armed attack (rather than cyber activities that fall below that threshold). At the same time, it highlights the particular importance of State practice in adopting and expounding the use of the "unwilling or unable" test in the cyber context. Indeed, news reports suggest that the United States is wrestling mightily to determine when it is appropriate and lawful to take cyber action outside the boundaries of its own networks.[5] Establishing State-to-State expectations about what types of cyber activities will trigger what types of responses will provide important incentives for ostensibly neutral States to take steps to protect their computer networks while minimizing the likelihood of inter-State misunderstandings that lead to unnecessary conflict in the cyber or non-cyber realms.[6]

Part II describes the "unwilling or unable" test, including relevant factors that States should use in assessing whether another State has met that test. Part III applies those factors to the cyber context. Part IV considers how the U.S. government may be approaching these issues. Part V concludes.

II. THE "UNWILLING OR UNABLE" TEST

In the wake of the September 11 attacks, the United States concluded that it was in an international armed conflict with Al Qaeda, a non-State actor. Perhaps the most controversial aspect of this claim was the implicit argument that the United States therefore could use force against members of Al Qaeda anywhere they appeared. This concept resulted in the much-

("The 'means at a neutral's disposal' principle should be the test for a neutral's duty for belligerents' IW [information warfare] incursions; the neutral should be held to apply means at its disposal to detect and repel these incursions. Such being the case, the correlative right of a belligerent aggrieved by IW incursions should be that the belligerent may take such actions as are necessary in the territory of a neutral that is unable (or perhaps unwilling) to counter enemy IW force activities making unlawful use of that territory, a principle from the law of naval warfare.").

5. Ellen Nakashima, *Pentagon Proposes More Robust Role for Its Cyber-Specialists*, WASHINGTON POST, Aug. 9, 2012.

6. *See* OWENS ET AL., *supra* note 3, at 318 (explaining rationales behind legal regimes that regulate the development and use of certain kinds of weapons).

maligned idea of the "global war on terror." The United States later took care to clarify that its international armed conflict claim did not mean that it would use force in all countries in which members of Al Qaeda appeared. Rather, the United States asserted that it would only use force in those countries that either gave the United States consent to do so or were "unwilling or unable" to suppress the threat itself.[7] Nor is the United States the only State to employ the "unwilling or unable" test when evaluating the legality of using force against non-State actors in another State's territory. Israel, Russia and Turkey all have cited the test in recent years.[8] Scholars, too, have described the "unwilling or unable" test as the applicable test in this situation,[9] though some contest that the test has any status in international law.[10]

---

7. John B. Bellinger III, Legal Adviser, U.S. Department of State, Address at the London School of Economics: Legal Issues in the War on Terrorism (Oct. 31, 2006); Harold Koh, Legal Adviser, U.S. Department of State, Address at the Annual Meeting of American Society of International Law (Mar. 25, 2010).

8. *See* Deeks, *supra* note 1, at 486–87 (listing other States' claims).

9. *See, e.g.*, NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 42 (2010) (reciting the "unwilling or unable" test as the correct test for determining when a victim State may take measures against non-State actors in the territorial State); YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENSE 217 (3d ed. 2001) ("Extraterritorial law enforcement is a form of self-defence, and it can be undertaken by Utopia against armed bands or terrorists inside Arcadian territory, in response to an armed attack unleashed by them from that territory. Utopia is entitled to enforce international law extraterritorially only when Arcadia is unable or unwilling to prevent repetition of that armed attack."); Carsten Stahn, *Terrorist Acts as "Armed Attack": The Right to Self-Defense, Article 51 (1/2) of the UN Charter, and International Terrorism*, 27 FLETCHER FORUM OF WORLD AFFAIRS JOURNAL 35, 47 (2003); Greg Travalio & John Altenburg, *Terrorism, State Responsibility, and the Use of Military Force*, 4 CHICAGO JOURNAL OF INTERNATIONAL LAW 97, 116 (2003) ("[S]hould a State be unwilling or unable to prevent its territory from being used as a sanctuary or base of operations by a transnational terrorist organization, a State threatened with an imminent attack by such an organization may . . . engage in a self-defense use of force to deal with this threat."); Alberto Coll, *The Legal and Moral Adequacy of Military Responses to Terrorism*, 81 AMERICAN SOCIETY INTERNATIONAL LAW PROCEEDINGS 297, 305 (1987) ("[O]nce it becomes reasonably evident that the harboring State is unable or unwilling to act, the injured State should be free to use the minimum of force required to stop the terrorist threat."); Ian Brownlie, *International Law and the Activities of Armed Bands*, 7 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 712, 732 (1958) ("Military action across a frontier to suppress armed bands, which the territorial sovereign is unable or unwilling to suppress, has been explained in terms of legitimate self-defense on a limited number of occasions in the present century."); Tatiana Waisberg, *Colombia's Use of Force in Ecuador Against a Terrorist Organization*, 12 ASIL Insights (2008), *available at* http://www.asil.org/insights080822.cfm ("State practice and the UN Security Council's

Although this test plays a significant role in regulating the geography of an armed conflict (or the geographic location of a State's response to an armed attack), its precise substantive and procedural content remains unclear. Must the victim State request assistance from the territorial State before using force against the non-State actor in the territorial State? By what standards should the victim State evaluate the territorial State's proposed means to address the threat and its capacity to do so? In the context of an armed conflict, what level of threat justifies taking action, using the "unwilling or unable" theory? International law currently does not answer these questions.

As complicated as an "unwilling or unable" inquiry may be in the non-cyber context, it becomes even more complicated in the cyber context. First, it is far easier to employ the cyber infrastructure of third States for hostile ends than it is to employ the physical territory of those States to commit conventional hostile acts. States and non-State actors that are engaged in armed conflicts or that are intent on committing armed attacks tend to operate from a single State or from a limited number of States, by virtue of cost, politics, logistics and terrain. In contrast, those same States and non-State actors are able to employ the cyber infrastructure of a much larger number of third States in forcible pursuit of their goals. Second, the difficulty of attribution in the cyber context is well-known.[11] As a result, there will be many situations in which the victim State can ascertain that a third country's servers are being used for hostile purposes but be unable to identify with certainty the actual authors of the attacks. In some cases, the victim State may not even be able to identify the geographic origin of a given cyber attack.[12] This stands in contrast to kinetic activities outside the cyber context, where the victim State often is able to identify the authors of the armed attacks and their locations, using well-established intelligence and investigatory resources. Third, the increased anonymity of cyberspace

---

actions after the September 11 attacks may, however, indicate a trend toward recognizing that a State that suffers large-scale violence perpetrated by non-State actors located in another State has a right to use force in self-defense when . . . that other State proves unwilling or unable to reduce or eliminate the source of the violence.").

10. *See* Kevin Jon Heller, *The Unwilling or Unable Standard for Self-Defense*, OPINIO JURIS, (Sept. 17, 2011), http://opiniojuris.org/2011/09/17/the-unwilling-or-unable-standard-for-self-defense-against-non-State-actors/ (rejecting "unwilling or unable" test as customary international law on basis that there is insufficient State practice and evidence of *opinio juris*).

11. *See, e.g.*, Jack L. Goldsmith, *The New Vulnerability*, NEW REPUBLIC (June 7, 2010).

12. OWENS ET AL., *supra* note 3, at 294.

may mean growth in the number of actors that seek to use cyber attacks. The deterrence that accompanies the fear of getting caught is reduced because the chance of being held accountable is lower.

Before turning to the cyber scenarios in which a State will need to employ the "unwilling or unable" test, however, it is important to clarify several assumptions in this article. First, this piece assumes that cyber attacks that produce effects similar to those of kinetic military actions will constitute "armed attacks" that trigger the victim State's right of self-defense.[13] Second, it assumes that non-State actors may be authors of armed attacks, even when those attacks are not attributable to a State.[14] Third, it assumes that, in the context of an international armed conflict, it would not violate the law of neutrality for a neutral State to allow a belligerent State to use, or not prevent it from using, its public internet and communications networks as a conduit for a cyber attack.[15] It assumes, however, that neutrality law would prohibit a neutral State from allowing a State or non-State actor to use its tangible computer equipment or operating systems, including servers, to host those attacks.[16] This means that a victim State, in responding to

---

13. *See, e.g.*, Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 929 (1998–99) (discussing possibility that computer network attacks could constitute "armed attacks"); Nils Melzer, *Cyberwarfare and International Law* 13, UNIDIR Resources (2011) (stating that cyber operations have the qualitative capacity to qualify as an armed attack within the meaning of UN Charter Article 51).

14. *See* Deeks, *supra* note 1, at 492–93 (describing three schools of thought on this question).

15. This follows from Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons during War on Land, art. 8. Oct 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague V], which States that a neutral power is not required to "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

16. *Id.* Allowing particular servers within the neutral State to host attacks is more closely akin to allowing a belligerent to move munitions of war across neutral territory or furnishing military supplies to a belligerent, which Hague V would prohibit. This seems to be the approach taken by the U.S. Department of Defense in 1999 in its Assessment of International Legal Issues in Information Operations. That document provides, "[U]se of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty . . . . A transited State would have somewhat more right to complain if the attacking State obtained unauthorized entry into its computer systems as part of the communications path to the target computer. It would be even more offended if malicious logic directed against a target computer had some harmful effect against the transited State's own equipment, operating systems, or data." *See also* TALLINN MANUAL, Rule 92 (Michael Schmitt ed., forthcoming 2013); Eric Jensen, *Sovereignty and Neutrality in*

a cyber armed attack against it, would not violate Article 2(4) simply by directing its response through a third State's public communications channels. The victim State would trigger Article 2(4), however, if it damaged a server hosted in that third State.[17] Fourth, it assumes that the victim State will be able to direct its response in a manner consistent with both the *jus ad bellum* and the laws of armed conflict, including the principles of distinction and proportionality.[18] Finally, it assumes that, as a matter of policy, the victim State will conduct its responses to a cyber armed attack in the cyber realm, although there is no legal requirement that it do so.[19]

There are at least three scenarios in which a State that has suffered a cyber attack may seek to take responsive (forcible) action in a third State's territory and therefore will need to assess the third State's willingness and ability to take action to address that cyber attack. First, a State may be fighting another State in an international armed conflict, where the State's opponent has launched a cyber attack from a third State's territory. In international armed conflict, the laws of neutrality apply. Assuming that the third State is neutral in the international armed conflict, the laws of neutrality require the neutral State to prevent its territory from being used by a belligerent as a place from which to launch attacks.[20] If a belligerent nevertheless is initiating or conducting cyber attacks against another belligerent using the cyber infrastructure of a neutral State, the neutral State must

---

Cyber Conflict, 35 FORDHAM INTERNATIONAL LAW JOURNAL 815, 826–27 (2012) (arguing that the law of neutrality would require a neutral State to prevent a belligerent from initiating or facilitating an attack within neutral territory, but not to prevent the mere passage of malware or malicious code over its public cyber infrastructure); Melzer, *supra* note 13, at 20 (reasoning that neutral States can be expected to prevent belligerents from conducting "cyber hostilities" from within neutral territory but not the "routing of belligerent cyber operations through their publicly accessible communications infra-structure"); *but see* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARVARD INTERNATIONAL LAW JOURNAL 179, 210 (2006) (arguing that even allowing the transit of malicious code over a State's public internet infrastructure would violate that State's neutrality obligations).

17. Such an act would be akin to severing a telephone wire in a State, interrupting general telecommunications in that State.

18. Whether this requires the victim State to identify with certainty the nature and identity of the cyber attacker is not clear.

19. The U.S. cyber security strategy preserves the right to respond kinetically to a cyber armed attack. However, given the level of caution with which the U.S. government seems to be proceeding in crafting doctrine for cyber responses, it seems reasonable to assume that using kinetic force against a cyber armed attack, particularly in a third State's territory, would occur only in an extreme case.

20. Hague V, arts. 2, 4; TALLINN MANUAL, *supra* note 16, at Rule 93.

make efforts to terminate that use. If the neutral State is unwilling or unable to stop that belligerent, the belligerent's opponent may take forcible measures within the neutral State to do so.[21]

Second, a State may be in a non-international armed conflict, fighting against a non-State actor whose operations are primarily based either within that State or within a foreign State's territory. The non-State actor may undertake cyber actions during that conflict that utilize systems located in foreign States. In this case, one may reason by analogy to the law of neutrality to assert that the State fighting the non-international armed conflict may take measures in that foreign State to suppress the non-State actor's cyber attacks where the foreign State is unwilling or unable to do so itself.[22] The United States appears to believe that this is the appropriate test to apply in the context of kinetic armed conflicts against non-State actors that transcend a single State's borders.[23] It is not clear whether a victim State could respond forcibly to *any* cyber uses of force emanating from the third State, or if the victim State only could respond forcibly to those cyber uses of force that rise to the level of a cyber armed attack.[24]

---

21. *See* SPAIGHT, *supra* note 2, at 482; John Norton Moore, *Legal Dimensions of the Decision to Intercede in Cambodia*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 38, 51 (1971) ("It is well established in customary international law that a belligerent Power may take action to end serious violations of neutral territory by an opposing belligerent when the neutral Power is unable to prevent belligerent use of its territory . . . ."); TALLINN MANUAL, *supra* note 16, at Rule 94.

22. Melzer, *supra* note 13, at 21 ("Strictly speaking, the law of neutrality applies only in international armed conflict. Arguably, however, the pragmatic logic of its core principles has already found its way into the practice of non-international armed conflicts as well."); International Committee of the Red Cross Official Statement of 8 March 2001 to the United Nations High Commissioner for Refugees Global Consultations on International Protection ("It is the ICRC's view that [Hague Convention V] can also be applied by analogy in situations of non-international armed conflicts, in which combatants either from the government side or from armed opposition groups have fled into a neutral State.").

23. Koh, *supra* note 7; John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Address at Harvard Law School: Strengthening Our Security by Adhering to Our Values (Sept. 16, 2011), http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an.

24. The United States generally asserts that virtually all uses of force constitute armed attacks that trigger a State's right of self-defense. *See* William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 299 (2004) (rejecting idea that attacks must rise to certain level of severity in order to qualify as armed attacks). Many States disagree with that position, however, and thus would have to confront how to respond to a use of cyber force short of an armed attack, launched by a non-

Third, a State that is not fighting an ongoing non-international armed conflict nevertheless may suffer a cyber armed attack from a non-State actor (or face an imminent threat thereof). This armed attack would trigger the victim State's right of self-defense under Article 51 of the U.N. Charter.[25] The victim State would then have to assess whether it was necessary to use force in self-defense against that non-State actor and, secondarily, whether it was necessary to use force *in that particular foreign State* against that non-State actor. If the territorial State is both willing and able to suppress the threat posed by that actor, it would not be necessary (and therefore would not be lawful) for the victim State to use force within the territorial's borders.

In each of these three scenarios, the victim State will be required to examine whether the territorial State can and will take action to halt or mitigate the attacks affecting the victim State. Although the test itself has traction in international law, its lack of substantive and procedural content makes it harder to apply and less legitimate as a restraining force in international relations. I previously suggested five principles, drawn from historical practice, that would help guide the test's application. These principles include the requirements that the victim State (1) prioritize cooperation or consent with the territorial State, rather than unilateral use of force; (2) ask the territorial State to address the threat and give it adequate time to respond; (3) reasonably assess the territorial State's capacity and control within the relevant region; (4) reasonably asses the territorial State's proposed

---

State actor extraterritorially. Those States might conclude that, absent an armed attack that triggers Article 51, the States cannot take any action in response that would violate Article 2(4) of the Charter. In practice, the United States actually may be imposing policy constraints on itself that bring it closer to that position. In his Harvard speech, John Brennan noted that "[b]ecause we are engaged in an armed conflict with al-Qa'ida, the United States takes the legal position that . . . we have the authority to take action against al-Qa'ida and its associated forces without doing a separate self-defense analysis each time." However, he also stated, "In practice, the U.S. approach to targeting in the conflict with al-Qa'ida is far more aligned with our allies' approach than many assume. This Administration's counterterrorism efforts outside of Afghanistan and Iraq are focused on those individuals who are a threat to the United States, whose removal would cause a significant – even if only temporary – disruption of the plans and capabilities of al-Qa'ida and its associated forces. Practically speaking, then, the question turns principally on how you define 'imminence.'" Brennan, *supra* note 23.

25. In the context of scenarios 2 and 3, "any action taken against [non-State actors] may raise issues about violating the sovereignty of that nation and its rights and obligations with respect to terrorist operations from or through its territory." OWENS ET AL., *supra* note 3, at 274.

means to suppress the threat; and (5) evaluate its prior interactions with the territorial State. Part III takes up these factors and applies them in the context of cyber attacks.

III. APPLYING THE TEST'S FACTORS TO CYBER ATTACKS

A. Preference for consent or cooperation

In the ideal situation, a victim State will approach the territorial State and inform the latter of the fact of the imminent or actual armed attack and its reasons for believing that the attacker is employing the victim State's infrastructure to commit the attacks. It then will seek consent to take action (whether forcible or not) to suppress the attacks emanating from the territorial State's computer systems. When it acts pursuant to and consistent with that consent, the victim State will not violate Article 2(4) of the Charter or the customary principle of non-intervention. Examples of such consent are not hard to find, particularly outside the cyber realm: Iraq previously allowed Turkey to use force in Iraq against a Kurdish terrorist group (the Kurdistan Workers' Party), and the United States reportedly is using force in Somalia and Yemen against members of Al Qaeda and associated forces with the consent of those governments.[26] Even if the territorial State is reluctant to let the victim State operate alone in its computer systems, there may well be opportunities for the two States to work cooperatively to suppress the threat.

This approach has several advantages. First, it minimizes the chance of cyber clashes between the victim and territorial States, and reduces the likelihood that those States find themselves working at cross-purposes against the cyber attacker. Second, this type of cooperation has the potential to enhance the victim State's own operations, to the extent that the territorial State has a deeper knowledge of its own computer systems, relationships with private sector companies whose computers the attacker may be using to facilitate the attack, and relevant information about past penetrations into the victim (or territorial) State's systems. Third, this cooperation and the corresponding information that it receives from the territorial State may help the victim State limit the collateral damage from its response, a

26. Scott Shane, *Yemen Sets Terms of a War on Al Qaeda*, NEW YORK TIMES, Dec. 4, 2010, at 1; U.S. Department of State Cable 09 NAIROBI 1057 ("Somalia TFG Prime Minister Worried About Rival") (Somalia).

constant concern in the cyber context.[27] The advantages of cooperation here may be more modest than in the more traditional context in which non-State actors conduct physical attacks against the victim State, however. In that context, local knowledge about terrain, terrorist camp locations and politics may prove particularly helpful in addressing the kinetic threats posed by terrorist or rebel groups. One disadvantage to obtaining consent or cooperation is temporal: in many cyber cases, a State may need (or wish) to respond to an ongoing attack immediately, leaving no time to seek a cooperative approach with the territorial State. One way to mitigate this temporal concern, while also promoting cooperation between the territorial and victim States, would be to negotiate consent agreements in advance.[28] In these agreements, the territorial State could provide advance consent to victim State operations in the former's cyber networks when certain triggers are met.

At the same time, the anonymity of cyber activity and the ease with which an actor may cover his tracks may reduce the victim State's overall incentives to seek any type of consent or cooperation from the territorial State before penetrating its cyber systems. In the cyber context, the victim State's actions in redress are less likely to come to light and, even if they do, it is easy for the victim State credibly to deny that it was the actual actor in that case.[29] In the non-cyber context, it is difficult (though not impossible) for a victim State physically to penetrate and use force in a territorial State without being detected. For example, an international investigation into the Cheonan incident (in which North Korea torpedoed a South Korean Navy ship) readily revealed Korean markings on the torpedo fragments.[30] In addition, the territorial State may be reluctant to cooperate with the host State

27. *See, e.g.*, Nakashima, *supra* note 5 (discussing U.S. concerns that actions in another country's networks could result in unintended consequences, including the disruption of civilian networks).

28. By way of precedent, the United States has negotiated a number of bilateral agreements relating to operations and ship-boarding to suppress the movement of narcotics and weapons of mass destruction. The latter set of agreements provides advance consent for either party to board a vessel flagged to the other party if the vessel is suspected of carrying illicit shipments of weapons of mass destruction. *See, e.g.*, Emma L. Belcher, *The Proliferation Security Initiative: Lessons for Using Nonbinding Agreements*, COUNCIL ON FOREIGN RELATIONS SPECIAL REPORT (July 2011).

29. *See* OWENS ET AL., *supra* note 3, at 81 (noting that most cyber attacks are inherently deniable).

30. Letter from the Permanent Representative of the Republic of Korea to the United Nations Addressed to the President of the Security Council (S/2010/281), June 4, 2010.

for national security reasons, particularly where the territorial State does not want to disclose information about its networks, systems and technology.

From a legal perspective, obtaining consent is an ideal way to avoid having to answer the host of difficult legal questions that currently attach to offensive and defensive uses of cyber tools. Action pursuant to consent also makes it less important that the victim State have a firm sense of who the author of the attacks is, because the territorial State is less likely to challenge the victim State's actions. From a political and military perspective, however, the costs of acting without seeking territorial State consent appear far lower than in the non-cyber context.

B. Request to address the cyber attack

Assume that the territorial State has not affirmatively consented to the victim State's use of cyber (or kinetic) tools to suppress the cyber threat emanating from the territorial State, perhaps because it is concerned about allowing the victim State to access its computer networks. At this point, the most direct way for a victim State to assess the territorial State's willingness and ability is to ask it to terminate the threat. Not only will this clearly put the territorial State on notice of the cyber attack, but it also will place an onus on the victim State to share relevant intelligence about the attack. If the territorial State responds by providing a plan for suppressing the attack, the victim State then has the basic information it needs to begin to assess the territorial State's willingness and ability to act.

Governments almost certainly will demand a caveat to this requirement, however. Where the victim State believes that the territorial State is colluding with the author of the cyber attack or will tip off the cyber attacker, the victim State should not be obligated to ask the territorial State before taking measures in the territorial State. This is a serious concern with States such as Russia and China, which are reported to use civilian proxies to conduct cyber attacks.[31] It is a particular concern in the cyber context because a hostile actor tipped off by the territorial State easily may divert its attacks through a different third State. Doing so in the non-cyber context takes time and money and poses significant logistical challenges.

31. Paul Rosenzweig, *From Worms to Cyber War*, DEFINING IDEAS, Dec. 9, 2011, http://www.hoover.org/publications/defining-ideas/article/102401 (describing Russian "cyber patriots"); David E. Sanger, John Markoff & Thom Shanker, *U.S. Plans Attack and Defense in Web Warfare*, NEW YORK TIMES, Apr. 28, 2009, at A1.

Creating too robust a caveat to the requirement to request assistance, however, will erode the balance that the "unwilling or unable" test strikes by putting a heavy finger on the scales in favor of security over sovereignty.

Even where the victim State is not concerned about a link between the territorial State and the hostile cyber actors, this factor magnifies complications that already exist in the non-cyber context. For the victim State, a requirement that it inform the territorial State about the cyber attacks it is suffering is not onerous. However, if the territorial State seeks additional information about those attacks—Are you sure they are coming from our territory? How do you know? What cyber tools do you have that can detect that, and how reliable are they?—the victim State may be hesitant to reveal its technological capacities.[32] Consider the territorial State's point of view as well. If the victim State simply asks it to suppress the threat, without seeking information about how the territorial State will do so, the territorial State may willingly comply, without having to reveal its cyber tools to the victim State. If the victim State seeks technological details about how the territorial State plans to proceed (which it reasonably might do to assure itself that the attacks will stop), the territorial State may be loath to reveal those details.[33] In the non-cyber context, it is far more likely that States will have adequate intelligence about each other's military hardware and capabilities. In the cyber context, the political relationship between the victim and territorial States—and, concomitantly, their willingness to share intelligence and technology—becomes highly predictive of how the victim State will proceed.

C. Good faith assessment of territorial State control and capacity

In the non-cyber world, when analyzing a territorial State's ability to suppress the threat, a victim State should assess what level of control the territorial State has over the geographic area from which the attacks are emanating. Conventional attacks plotted and launched from within a capital city may be far easier to detect, locate and suppress than attacks launched from remote jungles far from any town. A related question goes to the capacity of the territorial State's law enforcement and military officers, and

32. *See* Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 425 (2011) ("[N]o governments speak in much detail about their cyberwarfare capabilities and strategies at this point.").

33. As States garner increasing amounts of intelligence on each other's capabilities, this concern may diminish.

whether there are any reasons that those actors would not be able (or willing) to act against the non-State actors. In the cyber context, the question becomes how technologically sophisticated is the territorial State? While it is possible that one or more hostile actors is physically present in the territorial State, it is more likely that those committing cyber attacks against the victim State are present only electronically in the territorial State. Stopping those attacks, therefore, depends both on the capacity of the territorial State's cyber gurus and on the attacker's level of technical sophistication.

There is not enough publicly available information to gauge how often a victim State is likely to encounter a territorial State that is technically unable to defeat a cyber attack against the victim State. Some reports suggest that cyber is the great equalizer, allowing States with far weaker conventional militaries to take on those with traditionally strong conventional militaries.[34] Others assert that the cyber capacities of States such as the United States, Russia and China far exceed those of most other States.[35] Putting aside the objective capabilities of a particular territorial State, the secondary question of how much the victim State knows about the territorial State's capabilities remains a tricky one as long as cyber-capacities remain closely-held secrets. Publications such as *Jane's Defence Weekly* (as well as a State's domestic intelligence reports and the fact that States such as the United States may have provided weapons and training to the territorial State in question) make it relatively easy to ascertain what a State's kinetic capabilities are. In the cyber context, though, it will be particularly challenging for a victim State to assess the control and capacity of another State with which it does not have a close relationship already.

D. Good faith assessment of the territorial State's proposed means to suppress threat

Closely related to an assessment of the territorial State's capacity and control is a good faith assessment of the proposed means by which the territorial State will suppress the threat. The victim State must assess those pro-

34. Waxman, *supra* note 32, at 451, 455 (noting that "some experts assess that the United States is currently strong relative to others in terms of offensive capabilities" but also that "some States that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers").

35. Leon Panetta, U.S. Secretary of Defense, Remarks on Cybersecurity (Oct. 11, 2012) ("It's no secret that Russia and China have advanced cyber capabilities."), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

posed actions objectively. Even if the victim State would prefer to act itself, it should accept the territorial State's proposed approach if a "reasonable State" would believe that the approach will accomplish the victim State's core goal of suppressing the attack or threat of imminent attack.

In the non-cyber context, weeks may elapse between the time a territorial State proffers an operational plan and the time it executes it. In contrast, there will be almost immediate feedback on the success or failure of the territorial State's efforts to suppress the cyber threat. This makes it even more reasonable to defer to the territorial State's plan in the first instance, unless the ongoing attack against the victim State is so significant that there is no time for trial and error.

Establishing a preference for the territorial State's proposal is not without costs. Assume the territorial State proposes simply to shut off the server that is hosting the attacks against the victim State. Assume further that, if the territorial State permitted the victim State to address the threat itself, the victim State could stop the attack in a way that would allow it to continue to gather intelligence about the attacker. Should we continue to favor the territorial State's reasonable plan, even where doing so may force the victim State to lose some modicum of intelligence about its attacker? Probably so, though reasonable minds may disagree. What if the territorial State's plan is reasonable but is likely to result in some level of collateral damage, while the victim State has a high level of certainty that its plan would produce no such damage? In that case, the victim State would have at least a credible argument that the territorial State was "unable" to suppress the threat in a responsible way. Difficult questions such as these abound.

E. Prior interactions with the territorial State

Finally, in assessing the territorial State's proposed means to address the threat itself, the victim State should consider past interactions with the territorial State. Has the territorial State previously suppressed threats (conventional or cyber) emanating from its territory? Has the territorial State revealed a level of technical competence in the past that should give the victim State comfort that its proposed approach will work this time? Is the territorial State one from which cyber attacks consistently emanate, or is this an unusual incident? The more historically reliable and responsive the territorial State is, the less justification the victim State will have if it choos-

es to take action itself, and the more difficult it will be for the victim State to defend its actions if they come to light.

IV. ADVANCING CYBER LAW?

The United States has asserted that it will treat hostile acts in cyberspace as it would "any other threat to our country" and that it reserves the right to employ a military response, "as appropriate and consistent with applicable international law."[36] In other statements, the United States has made clear that in the non-cyber context, international law allows the United States to use force against non-State actors in another State's territory only when the territorial State has consented or is unwilling or unable to suppress the threat.[37] This—coupled with multiple news reports about internal debates within the U.S. government on cyber questions[38]—suggests that the United States is attempting to reason by analogy from existing international law governing the *jus ad bellum*. These reports also suggest that the United States is attempting to craft appropriate, and apparently highly restrictive, operational rules of the road in the cyber sphere. One news report stated that U.S. officials are focused on "concerns that action in another country's networks could violate international law, upset allies or result in unintended consequences, such as the disruption of civilian networks."[39] The article further reported that the U.S. Department of Defense has developed "strict conditions governing when military cyber-specialists could take action out-

36. THE WHITE HOUSE, U.S. INTERNATIONAL STRATEGY FOR CYBERSPACE 14 (May 1, 2011); Harold Koh, "International Law in Cyberspace," USCYBERCOM Interagency Legal Conference, Sept. 18, 2012.

37. Brennan, *supra* note 23 ("The United States does not view our authority to use military force against al-Qa'ida as being restricted solely to 'hot' battlefields like Afghanistan. Because we are engaged in an armed conflict with al-Qa'ida, the United States takes the legal position that—in accordance with international law—we have the authority to take action against al-Qa'ida and its associated forces without doing a separate self-defense analysis each time. And as President Obama has stated on numerous occasions, we reserve the right to take unilateral action if or when other governments are unwilling or unable to take the necessary actions themselves.").

38. *See, e.g.*, Nakashima, *supra* note 5; Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response and Debate Over Dealing with Threats*, WASHINGTON POST, Dec. 8, 2011.

39. Nakashima, *supra* note 5. It is not clear whether those contemplated U.S. actions would be forcible or would consist of actions short of force (such as non-forcible countermeasures).

side U.S. networks" and that those conditions "are so stringent that the new capability to go outside military boundaries might never be used."[40]

In some ways this U.S. process is puzzling. In the face of such legal and technological uncertainty, one might expect a country with extensive cyber capabilities to take a minimalist approach to legal compliance, at least until the international community formulated certain common understandings about how to approach cyber warfare. Indeed, in the non-cyber context, the U.S. Government has done less hand wringing about using force extra-territorially, even though the manifestation of that force is far more public. Why is the United States working so hard to find the law and apply it in the cyber realm, where violations of Article 2(4) would be both legally uncertain and difficult to detect?

There are at least five factors that may explain why the United States has been edging cautiously toward a relatively constraining legal regime (one that in all likelihood will be a unilateral approach for some time to come). First, there often is an inherent institutional instinct in the U.S. government to anchor novel legal situations in existing bodies of law and practice, and to reason by analogy. This is, after all, the approach the Obama administration took toward detainee habeas cases.[41] There, the government determines (and asks courts to affirm) that someone is a combatant based on functional analogies between that person's activities and the activities of a member of a State's armed forces. Particularly where the analogies are quite reasonable (as they are between kinetic and cyber activities), it often is easier to draw from existing rules than to craft new ones from whole cloth. Additionally, U.S. government lawyers know that other governments are

40. *Id.* (noting that shutting down a server in another country likely would require Presidential permission). *See also* David Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses*, New York TIMES, Apr. 27, 2009 (stating that President Bush personally authorized penetration by the U.S. military of a computer in Iraq to lure Al Qaeda members into an ambush); Ellen Nakashima, *Pentagon Considers Preemptive Strikes as Part of Cyber-Defense Strategy*, WASHINGTON POST, Aug. 28, 2010 (reporting on internal U.S. government debate about when the United States may go into foreign cyberspace and take preemptive action).

41. Respondent's Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantanamo Bay, In re: Guantanamo Bay Litigation, Mar. 13, 2010 (stating that the President has the authority under the 2001 Authorization for Use of Military Force to detain those persons whose relationship to Al Qaeda or the Taliban would, in appropriately analogous circumstances in a traditional international armed conflict, render them detainable).

likely to use those existing rules as a starting point from which to evaluate U.S. action.[42]

As a related matter, the U.S. culture surrounding the use of force and the conduct of armed conflicts has grown increasingly legalistic in the past ten years. While the United States always has been conscious of the legal role that the UN Charter plays in regulating uses of force, the past decade has found lawyers playing a particularly prominent role in structuring government decision making in this area.[43] A robust interagency process within the National Security Council ensures a forum for voices (such as those from the State Department) that are concerned about the diplomatic and reputational impacts of cyber activities that are seen as unlawful or illegitimate. And a perennial interest in being seen as following the rule of law renders unappealing an approach that ignores legal constraints entirely.[44]

Third, the United States is keenly aware of the ongoing controversy about its geographic approach to the U.S. conflict with Al Qaeda and associated forces.[45] The notion that the United States takes a forward-leaning approach to using force in third States with which it is not in conflict remains uncomfortable and legally contentious for many States. It follows that the United States would be similarly attuned to the far greater number of States that may (advertently or inadvertently) host cyber attacks against it, and to the almost-certain controversies that would follow from its uses of cyber (or kinetic) force in those States, absent a robust and well-articulated legal defense of those actions. Developing cautious standards through a cautious process is one way to establish that defense and to place other States on notice of its contents.

---

42. Matthew Waxman suggests that this is not the only approach that the United States might have taken. Waxman, *supra* note 32, at 453 (noting that it might be "in the United States' strategic interest to legally *delink* cyber-activities from armed force instead of defining force by reference to effects").

43. For a discussion of the role of international law in the Cuban Missile Crisis, *see* ABRAM CHAYES, THE CUBAN MISSILE CRISIS (1974). For the lawyers' role in the past ten years, *see* JACK GOLDSMITH, POWER AND CONSTRAINT xv (referring to "faceless executive-branch lawyers" micromanaging national security decisions).

44. Brennan, *supra* note 23 (describing one of the core values of the United States as "adhering to the rule of law").

45. *Id.* ("An area in which there is some disagreement is the geographic scope of the conflict. The United States does not view our authority to use military force against al-Qa'ida as being restricted solely to 'hot' battlefields like Afghanistan. . . . Others in the international community—including some of our closest allies and partners—take a different view of the geographic scope of the conflict, limiting it only to the 'hot' battlefields.").

Even assuming these three propositions are true, this does not explain why the United States has not chosen to adopt freedom of action in cyberspace—at least for now, while the law is very unclear and it remains difficult to attribute a particular cyber action to any particular actor. That is, if the United States felt that it were justified in responding to a particular incoming attack—even one with origins in a friendly and technologically advanced State—why would it not simply respond to the attack in that friendly State and then deny knowledge of the response? One answer seems to lie in concerns about cyber collateral damage.[46] Past efforts to dismantle particular websites have resulted in unexpected disruptions of servers in various countries. For instance, when the U.S. military dismantled a Saudi web site in 2008, it inadvertently disrupted over 300 servers, including in Texas, Saudi Arabia and Germany.[47] The high likelihood of collateral damage (and the concomitant likelihood that such damage becomes public) may place significant pressure on a country such as the United States to set a prudentially high bar for using cyber force in other States' territories.[48]

Finally, reciprocity concerns echo loudly in the ears of U.S. policymakers and lawyers. Even though the United States rarely will find itself being accused by other States of being unwilling or unable to suppress a particular cyber threat, the United States should be interested in prioritizing consent wherever possible, to create an expectation that other States affected by cyber attacks emanating from the United States will approach the U.S. government in the first instance, before taking unilateral action against U.S. cyber infrastructure.[49] This is particularly true because the United States is viewed as a major source of cyber attacks, cyber exploitations and botnets.[50] It is not in the U.S. interest to allow other States to claim that there is a legal black hole regarding cyber uses of force or to be able to

---

46. *See* OWENS ET AL., *supra* note 3, at 121–26 (describing difficulty in calculating accurately collateral damage from a cyber attack and describing damage assessment techniques for cyber attacks as "primitive").

47. Nakashima, *Preemptive Strikes*, *supra* note 40.

48. Note that this is true even if the United States is in an international armed conflict with State X and wishes to use cyber force against computers located within State X. Even that activity, which does not implicate the "unwilling or unable" test, may lead to collateral damage in third States.

49. It seems much more likely that a State would contemplate using unilateral cyber force against the United States than using unilateral kinetic force against it.

50. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View* 7, HOOVER INSTITUTE, media.hoover.org/documents/FutureChallenges_Goldsmith.pdf (last visited Oct. 28, 2012).

claim that the "unwilling or unable" test has no substantive or procedural content.

V. CONCLUSION

The "unwilling or unable" test remains a relevant proposition when a victim State suffers a cyber armed attack that is launched from the territory of a non-hostile State. Depending on the kinds of cyber activities that States treat as violating a neutral State's obligations and those that they treat as rising to the level of an armed attack, the international community will employ the test more or less frequently. The nature of cyber attacks—including the speed at which they occur—places pressure on the victim State to conduct both a rapid and accurate assessment of the territorial State's capabilities and political disposition. Cyber attacks also place pressure on the territorial State to reveal some of its technological capacity if it wishes to avoid having the victim State act in its stead. The relationship between the territorial and victim States will play an outsized role in the outcome of the "unwilling or unable" inquiry. Yet this inquiry stands between the victim State and a "global cyberwar on terror," and must be taken seriously.