FLETCHER SECURITY REVIEW

Security Challenges & Opportunities in the Next American Century: *A Conversation with* **David H. Petraeus**

Ukraine - Europe's New Proxy War?
Geraint Hughes

Proxy Wars in Cyberspace
Michael N. Schmitt & Liis Vihul

Purveyors of Terror
Thomas Dempsey

EDITORS

The *Fletcher Security Review* builds on the Fletcher School's strong traditions of combining scholarship with practice, fostering close interdisciplinary collaboration, and acting as a vehicle for groundbreaking discussion of international security. We believe that by leveraging these strengths – seeking input from established and up-and-coming scholars, practitioners, and analysts from around the world on topics deserving of greater attention – we can promote genuinely unique ways of looking at the future of security.

Letters to the Editor
Address letters to:
Editor in Chief, Fletcher Security Review
editor@fletchersecurity.org

Or by mail:
Suite 609 Cabot, Fletcher School
160 Packard Avenue, Medford, MA 02155

Information for Authors
Please send submissions to:
editor@fletchersecurity.org

All submissions should be sent as a Microsoft Word file. Short articles should be 1,500 to 2,000 words and long articles should be be 3,000 to 5,500 words.

Listings:
Columbia International Affairs Online

Proxy Wars in Cyberspace: The Evolving International Law of Attribution

Michael N. Schmitt & Liis Vihul

Introduction

The technical complexity of determining the perpetrators of cyber operations has resulted in a perception that states can operate with impunity in cyberspace. Clearly, the attribution challenge contributes to this perception by sometimes affording them a covert means of pursing national security objectives. Targeted states often find their response options limited in the absence of an identifiable state author of the operations. Moreover, the anonymity of many hostile operations also renders classic deterrence strategies anaemic in cyberspace.

Yet, the finger of culpability often points at states, whether fairly or not. Some of the most severe and notorious cyber operations against states have been associated with other states, even if very loosely so.[1] For example, the large-scale, distributed denial of service attacks against Estonia in 2007 were viewed by many as Russia's punitive response to the Estonian government's decision to relocate a World War II Soviet memorial. The attempted cyber espionage targeting the US military secret network (SIPRNET) in 2008 that prompted the creation of United States Cyber Command, as well as those taking place in the Georgia-Russia war the same year, were also seen as associated with Russia. The paradigmatic case is the use of the Stuxnet malware during Operation "Olympic Games," which has been widely, albeit unofficially, credited to Israel and the United States. More recently, Iran is believed to have carried out cyber attacks against US financial institutions (Operation Ababil) and used the Shamoon malware against Saudi Arabia's national oil company, Saudi Aramco, and Qatar's RasGas.

Today, it is incontrovertible that states carry out hostile activities against other states in cyberspace. Some states have gone so far as to publically express a strategic interest in doing so,[2] but most are understandably reticent to be identified as the source of any hostile cyber operations. The aforementioned technical difficulties of attribution serve a useful role in this regard. But to further attenuate the difficulty of attribution, a variety of non-state actors operate in this environment. While some pursue independent agendas, others act in varying degrees of support for particular states and their policy objectives. In some cases, they act as proxies for the states concerned.

1 For an excellent review of State and non-State activities in cyberspace, see Kenneth Geers et al., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks* (FireEye Labs), accessed January 31, 2014, http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf.

2 See, e.g., *The Defence Cyber Strategy* (Netherlands Ministry of Defence), 5, 6, 8, 11, accessed January 31, 2014, http://www.defensie.nl/_system/handlers/generaldownloadHandler.ashx?filename=/english/media/cyberbrochure_engels_tcm48-199915.pdf.

Since non-state cyber operations are often feasible at a fairly low cost and without access to the technical wherewithal of states, care has to be taken when presuming state sponsorship of non-state cyber activities. For example, the 2007 cyber operations targeting Estonia were in part attributable to the Nashi youth activist group, but it is unclear whether the Russian Federation had a hand in the group's operations.[3] Similarly, the aforementioned attacks on the US banking sector have been attributed primarily to the Izz ad-Din al-Qassam Cyber Fighters, a group that launched them in response to the YouTube release of the movie "Innocence of Muslims" and its alleged insult to the Prophet Mohammed. Whether the Iranian government played a part, and if so how, remains uncertain.[4] As these cases demonstrate, establishing a nexus between the actions of a non-state actor and the state itself can be a challenging endeavour.

This article examines the legal landscape of proxy cyber operations. The precise legal question is when may the cyber activities of a non-state group or individual, or even in some cases another state, be attributed to a state as a matter of international law. In order to answer this question, a multilevel legal analysis is required because the applicable legal norms that apply vary depending on the legal context of the attribution. The article discusses attribution in three contexts. First, it explores attribution for the purpose of establishing state responsibility for the actions of non-state groups. In other words, it answers the question of when is a state legally responsible for the actions of a non-state group's cyber operations such that it may have to act to halt the operations, pay reparations for damage, or be subject to the target state's "countermeasures," an exceptional remedy explained below. Second, it examines the preconditions to treating a cyber operation by a non-state actor as an "armed attack" mounted by its state sponsor, thereby allowing the victim state to respond forcefully in self-defense against that state itself (in addition to responding directly against the non-state group), as well as opening the door to a forceful response by other states, such as NATO member states, in collective defense. Finally, it assesses when state sponsorship of a non-state group results in the sponsor state becoming a party to an international armed conflict. In lay terms, when does state sponsorship of non-state cyber operations result in the two states being "at war"? This is a

3 Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: CCD COE Publications, 2010), 23-24; "Nashi Activist Says He Led Estonia Cyberattacks," *The Moscow Times*, March 13, 2009, http://www.themoscowtimes.com/news/article/nashi-activist-says-he-led-estonia-cyberattacks/375271.html.

4 Ellen Nakashima, "Iran Blamed for Cyberattacks on US Banks and Companies," *The Washington Post*, September 21, 2012, l; Jeb Boone, "Who Are the Izz Ad-Din Al-Qassam Cyber Fighters?" *GlobalPost*, November 9, 2012, http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/who-are-the-izz-ad-din-al-qassam-cyber-fighters.

crucial question because once an armed conflict exists, the law of war (international humanitarian law (IHL) governs the situation.

The Law of State Responsibility

The law of state responsibility is concerned with the legal consequences of a state's violations of international law. By this body of customary international law, which has been captured by the International Law Commission in its *Draft Articles on Responsibility of States for Internationally Wrongful Acts*,[5] states are

5 U.N. International Law Commission, Report of the International Law Commission, Draft Articles of State Responsibility, U.N. GAOR, 53rd Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001) [hereinafter Articles on State Responsibility]. The general international law of State responsibility has not been set forth in a treaty. Rather, it emerges as the product of State practice that is engaged in out of *opinio juris*, i.e. a sense of legal obligation (customary international law). The International Court of Justice has recognized customary law as a valid form of international law in the Statute of the International Court of Justice. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1055, T.S. No. 993, 3 Bevans 1179.

responsible for their "internationally wrongful acts" to those whom they have "injured" in the sense of violating an obligation owed.[6] Such acts are composed

> ***"Today, it is incontrovertible that states carry out hostile activities against other states in cyberspace."***

of two analytically distinct elements: 1) an act or omission that breaches an international legal obligation, and 2) attributability of the act to the "responsible state."[7] In the event the responsible state breaches an obligation owed to the injured state, it is obliged to immediately cease the offending conduct (an act) or comply with the required duty (an omission) and make full reparation to the injured state.[8] This system applies fully to state cyber operations that violate an international obligation owed to the target state. It is thus unquestionable that a state conducting a cyber operation that violates a treaty or customary international law duty to another state is under an obligation to immediately terminate the operation. It is equally clear that a state to which the cyber operations of a non-state actor are attributable is legally required to do everything in its power to stop them.

The law of state responsibility also provides for the taking of countermeasures in response to a continuing or unremedied breach of an obligation it is owed. Countermeasures are actions "which would otherwise be contrary to the international obligations of [an] injured state *vis-à-vis* the responsible state if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation."[9] Restated, the responsible state has breached, through an act of either commission or omission, a treaty or customary international law obligation owed to another state. The injured state may respond with action that would itself constitute a breach of an obligation owed to the responsible state – the countermeasure. Its response will not be considered internationally wrongful so long as it complies with the various requirements set forth for countermeasures in the law of state responsibility.[10]

6 Articles on State Responsibility, arts. 1, 28.

7 Ibid., art. 2.

8 Ibid., arts. 30(a), 31.

9 Ibid., para. 1 of chapeau to Chapter II.

10 Ibid., arts. 49-54. On countermeasures in the cyber context, see *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter Tallinn Manual], gen. ed. Michael N. Schmitt (New York: Cambridge University Press, 2013), Rule 9 and accompanying commentary; Michael N. Schmitt ""Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law," forthcoming *Virginia Journal of International Law* 54 (2014).

Countermeasures must be distinguished from acts of retorsion, which are "unfriendly" but not unlawful actions, such as an economic embargo or severance of diplomatic relations. Additionally, the sole purpose of a countermeasure is to force the responsible state into compliance with the law; retribution, punishment, and the like are impermissible objectives.[11] In the cyber context, countermeasures often represent an effective means of self-help by allowing the injured state to take urgent action that would otherwise be unavailable to it, such as "hacking back," to compel the responsible state to cease its internationally wrongful cyber operations. With respect to proxies, if the non-state actor's cyber operations are attributable to a sponsoring state as a matter of law, it is lawful to launch countermeasures at that state itself to compel it to use its influence to put an end to the non-state actor's operations.

With respect to the first prong of the test for an internationally wrongful act, the wrongfulness thereof, state cyber operations could violate many treaty (whether bilateral or multilateral) and customary norms of international law. Prominent among these is the prohibition on the use of force. As confirmed in the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, it is unequivocal that those cyber operations which cause injury or death of persons, or damage or destruction of property, violate the prohibition,[12] which is resident in customary law, as well as codified in Article 2(4) of the UN Charter, unless justified under the doctrine of self-defense or by UN Security Council authorization. Arguably, certain cyber operations that do not have destructive or injurious consequences would also qualify as a use of force.[13]

Since states are more typically the target of cyber activities of lesser gravity, the international community is paying increasing attention to other relevant international law norms prohibiting particular cyber behaviour by states.[14] The effort to clear the normative fog surrounding these norms in the cyber context has been hampered by a paucity of *opinio juris* – pronouncements by states that they are required to act or refrain from acting in a particular way due to the existence of a legal obligation.[15] Absent *opinio juris*, it is difficult to assess whether the community views particular actions as legally mandated

11 Articles on State Responsibility, para. 1 of commentary to art. 49.

12 Tallinn Manual, para. 8 of commentary to Rule 11.

13 Ibid., para. 10 of commentary to Rule 11.

14 The NATO CCD COE has launched a follow-on project to the Tallinn Manual titled "Tallinn 2.0". It examines the international legal issues surrounding cyber operations that fall below the "armed attack" threshold, and will result in a second, expanded edition of the Tallinn Manual in 2016.

15 On *opinio juris*, see North Sea Continental Shelf (Ger. v. Den.; Ger. v. Neth.), 1969 I.C.J. 3, para. 77 (Feb. 20).

(or forbidden) or as simply the product of policy decisions. This scarcity can be explained by the paradoxical situation states find themselves in with respect to cyber activities. On the one hand, IT-dependent states that are most vulnerable to hostile cyber activities have an incentive to characterize hostile cyber activities as violations of international law. On the other hand, IT-dependency often goes hand-in-hand with IT-capability; states that have developed an advanced cyber infrastructure are also the most likely to possess offensive cyber capabilities. Their reticence to openly style cyber operations against them as unlawful can be explained in part by a fear of limiting their own of courses of action in the future.

Despite this situation, there is no question that non-destructive or injurious malicious cyber operations can violate various established international law norms. Prominent among these are the principles of sovereignty and non-intervention. The principle of sovereignty empowers a state to "exercise control over cyber infrastructure and activities within its territory."[16] Correspondingly, the principle of sovereignty protects cyber infrastructure on a state's territory irrespective of whether it is government owned or private. The International Group of Experts that drafted the *Tallinn Manual* struggled with the application of the principle. All agreed that a cyber operation by another state that caused damage to cyber infrastructure violated the territorial state's sovereignty, whereas mere cyber monitoring did not.[17] They disagreed over whether placing malware into cyber infrastructure or altering or destroying data qualified as a violation. Importantly, the protective scope of sovereignty is limited to a state's territory (and government vessels and aircraft). By this logic, a cyber operation by State A that alters critical data stored in a server on State B's territory violates State B's sovereignty. However, if State B stored the same data in State C, State A's operation would only violate State C's sovereignty.

The international law prohibition of intervention in another state is centred on the element of coercion; an unlawful intervention occurs when a state intends to compel another state in its internal or external affairs (i.e. matters that are reserved to that state). The International Court of Justice has confirmed that the non-intervention principle is violated, for example, if a state provides "financial support, training, supply of weapons, intelligence and logistic support" to a terrorist or insurgent group operating in another state.[18] Thus, funding malicious cyber activities by such a group, training its members in cyber attack techniques, or supplying malware to the

16 Tallinn Manual, Rule 1.

17 Ibid., para. 6 of commentary.

18 Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, para. 242 (June 27) [hereinafter Nicaragua].

group would all qualify as intervention by the state sponsor.

These are only two examples of internationally wrongful acts below the use of force threshold for which states may be held responsible and that may open the door to demands for cessation, reparations, and the taking of countermeasures; others may derive from such areas of law as the law of the sea, international telecommunications law, space law, and, with respect to individuals, human rights law. Regardless of the legal obligation concerned, the breach has to be attributable to a state to result in state responsibility. Therefore, the salient question with respect to this article is: When are the acts of non-state actors attributable to states?

Obviously, the conduct of "state organs" of government, such as military, intelligence, and security agencies, is attributable to the respective state.[19] The law of state responsibility infuses the term "state organ" with a broad meaning to ensure that states cannot escape responsibility by asserting an entity's non-status as its *de jure* organ pursuant to domestic law. Such *de facto* organs are regarded as state organs for the purposes of state responsibility provided that they are completely dependent on the state and that dependency inherently provides for the state's potential complete control over them.[20] Therefore, cyber operations, whether in defense or offense, conducted by, for instance, the Netherlands Defence Cyber Command,[21] the French Network and Information Security Agency (ANSSI),[22] the Estonian Defence League's Cyber Unit[23] or the United States Cyber Command[24] are unquestionably attributable to their respective states. Indeed, their conduct is attributable even when the action is *ultra vires*, that is, unauthorized.[25]

Furthermore, sometimes persons or entities who are not state organs are permitted by the domestic law of a state to exercise elements of governmental authority. So long as they are acting in that capacity, their actions will be considered an act of that state.[26] For example, a private entity that issues certificates for national identification documents in order to assure the security and authenticity of legally binding digital signatures so qualifies.

19 Articles on State Responsibility, art. 4.

20 Nicaragua, paras. 109, 110. See also Marko Milanovi , "State Responsibility for Genocide," *European Journal of International Law* 17, no.3 (2006): 576-77.

21 *The Defence Cyber Strategy*, 11.

22 See the website of Agence nationale de la sécurité des systèmes d'information at http://www.ssi.gouv.fr/en/the-anssi.

23 See the website of Estonian Defence League's Cyber Unit at http://www.kaitseliit.ee/en/cyber-unit.

24 See, e.g., *Department of Defense Strategy for Operating in Cyberspace* (2011), 5, accessed January 31, 2014, http://www.defense.gov/news/d20110714cyber.pdf.

25 Articles on State Responsibility, art. 7.

26 Ibid., art. 5.

Before turning to the specific rules governing attribution of a non-state group's cyber activities, it is useful to distinguish between breach of an obligation by a state and its responsibility based on a non-state actor's cyber operations. For instance, international law dictates that a state may not "allow knowingly its territory to be used for acts contrary to the rights of other states,"[27] an obligation that applies fully to cyber infrastructure located on its territory.[28] A state would therefore be required to take down a botnet's command and control server located on its territory and used by a terrorist group to carry out a large-scale distributed denial of service attack (DDoS) against another state's critical cyber infrastructure, such as its electrical grid. Failure to do so is itself a breach by the state. But whether the state is responsible for the terrorists' DDoS attack is a question of attribution.

By the general rule, the conduct of governmental organs is attributable under international law, whereas the actions of private persons are generally not.[29] The conduct of non-state actors is only attributed to a state when they are either acting "on the instructions" of that state or acting under its "direction or control" (although not when the acts are *ultra vires*).[30] No requirement vis-à-vis the legal status of the person or group exists; they could include, for example, individual hackers, criminal groups, an informal group with its own identity like Anonymous, a legal entity such as the Microsoft Corporation, or terrorist or insurgent groups. The key is that unlike state organs, attribution of non-state actors' conduct is solely made based on the factual relationship between the person or group engaging in internationally unlawful cyber activities and the state.[31] Of particular note are state owned IT companies. Ownership by the state as such does not suffice for attribution. Instead, a company (assuming it is not exercising elements of governmental authority) must be acting under the instruction, direction, or control of the state before its cyber activities are attributable to that state.

Because the concepts of "acting on the instructions" and "acting under the direction or control" of a state have not been well-developed in the law of state responsibility, each case has to be assessed on its own merits. Acting "on the instructions" of a state is generally equated with conduct that is authorized by that state.[32] In other words, the non-state actor functions as the state's "auxiliary" in that the state has hired, recruited, or otherwise instigated it to act

27 Corfu Channel (U.K. v. Alb), 1949 I.C.J. 4, 23 (9 April) at 22.
28 Tallinn Manual, Rule 5 and accompanying commentary.
29 Articles on State Responsibility, paras. 2-3 of chapeau to Chapter II.
30 Ibid., art. 7.
31 Ibid., para. 1 of commentary to art. 8.
32 Ibid., paras. 2, 8 of commentary to art. 8.

in a particular way. For example, a state may employ a private company to steal military intellectual property whenever possible from another state. The company is acting on state instructions. So long as the theft violates an international legal obligation owed to the injured state (e.g., a provision of a treaty of amity and friendly relations between the states concerned), state responsibility arises.

The notion of "direction or control" is limited to the conduct of specific operations, rather than merely supplementing a state's activities or assuming responsibility for performing a particular function, as in the case of "instruction."[33] For example, a state may conclude a confidential contract with a private computer security company to program a back door into its encryption product, as was alleged with respect to the National Security Agency and the security company RSA.[34] Once that program is installed on another state's governmental computer, the state will direct the enterprise to exploit the back door and plant malware on that computer which will start extracting documents and forwarding them to the directing state. The company's behaviour is attributable to the directing tate, provided that the implantation of malware qualifies as a breach of the other state's sovereignty or amounts to another breach of an obligation owed to the target state. In this scenario, the injured state may accordingly demand cessation through removal of the malware, reparation, and assurances and guarantees of non-repetition.[35] So long as the state that contracted the specific activities has not complied with these obligations, the injured state may also engage in proportionate countermeasures against it.

"Before turning to the specific rules governing attribution of a non-state group's cyber activities, it is useful to distinguish between breach of an obligation by a state and its responsibility based on a non-state actor's cyber operations."

A critical issue is the requisite degree of control. The International Court of Justice, in a standard acknowledged by the International Law Commission, has stated that a state must exercise "effective control" over the non-state actor in question for state responsibility to

33 Ibid., para. 3 of commentary to art. 8.

34 Joseph Menn, "Exclusive: Secret contract tied NSA and security industry pioneer," *Reuters*, December 20, 2013, http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

35 Ibid., art. 30(b).

attach.[36] While this notion has not been defined, it presumes a higher level of participation than general or "overall" (see below) control by the state.[37] Merely encouraging or generally supporting non-state actors' cyber operations does not qualify, nor does having the ability to somehow influence the non-state actor's actions.[38] As an example, Russia's silent endorsement of the 2007 cyber attacks against Estonia, demonstrated, *inter alia*, by its refusal to assist Estonian authorities in related criminal proceedings pursuant to the Agreement on Mutual Legal Assistance, did not suffice to attribute the attacks to Russia.[39] In the context of a non-state actor's military operations, a state's preponderant or decisive participation in the "financing, organizing, training, supplying, and equipping [ ], the selection of its military or paramilitary targets, and the planning of the whole of its operation" has been found insufficient to meet the "effective control" threshold.[40] To satisfy the stringent effective control test, the non-state group must essentially be conducting its operations on behalf of the State.[41] Of course, the fact that the non-state group's activities are not attributable to the state does not mean that the state is not responsible for its own internationally wrongful act, such as intervention.

An additional basis for attribution of a non-state actor's cyber operations exists when the state "acknowledges and adopts the conduct in question as its own."[42] The International Court of Justice recognized this basis in the *Tehran Hostages* case. There, the Court found that Iran bore responsibility for holding US hostages between 1979 and 1981 because "[t]he approval given to [the seizure] by the Ayatollah Khomeni and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State." [43] Thus, for example, if a state expresses approval for particular non-state cyber operations against another state and subsequently acts to support them, as in mounting cyber defences to foster their continuance, the acts become attributable. However, this is a relatively limited basis for attribution. Merely expressing support or encouraging the non-state actors is insufficient.

These thresholds are very high. The

36 Nicaragua, para. 115; Articles on State Responsibility, para. 4 of commentary to art. 8.

37 Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro), 2007 I.C.J. 43, para. 406 (Feb. 26) [hereinafter Genocide].

38 Tallinn Manual, para. 10 of commentary to Rule 6.

39 Tikk, Kaska and Vihul, *International Cyber Incidents*, 27-28.

40 Nicaragua, para. 115.

41 Ibid., para. 109.

42 Articles on State Responsibility, art. 11.

43 United States Diplomatic and Consular Staff in Tehran (US v. Iran), 1980 I.C.J. 3, para. 74 (May 24).

more non-state actors turn to cyber operations, and the more their capabilities and sophistication grow, the greater the opportunities and incentives for states to covertly leverage them. This will result in an understandable temptation on the part of states that are the target of non-state cyber operations to interpret the thresholds liberally. However, a countervailing desire to avoid responsibility on the part of states employing cyber proxies will encumber development along these lines. In light of these competing incentives, the thresholds are likely to remain intact for the foreseeable future.

A related question is the requisite level of certainty that the state is involved for attribution to occur. In this regard, the state injured by the non-state actor bears the burden of proof that the latter's cyber operations are attributable to another state.[44] As to the standard of proof, the Iran-United States Claims Tribunal has held that both the identity of the originator as well as its association with a particular state must be proven with "reasonable certainty."[45] The mean-

44 Articles on State Responsibility, para. 8 of chapeau to Chapter V.

45 Kenneth B. Yeager v. The Islamic Republic of Iran, 17 Iran-US Cl. Trib. Rep. 92, 101-02 (1987). This position is also adopted in the Articles

ing of the notion "reasonable certainty" is context-dependent. In principle, the graver the underlying breach, the greater the confidence must be in the evidence relied upon.[46] This is because the robustness of permissible responses grows symmetrically with a breach's seriousness, particularly with respect to countermeasures. Such measures must comport with the requirement of proportionality; that is, they "must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[47] For instance, if non-state actors launch cyber operations on behalf of a state that cause some limited disruption, inconvenience, and irritation, it would not be lawful to respond against the responsible state with cyber operations that bring about large-scale economic loss or physical damage. Therefore, the requirement for confidence in the evidence increases as the risk of misattribution of activities to an "innocent" state intensifies.

The International Court of Justice has intimated the existence of a requirement for "clear evidence" in the case of attribution of a non-state group's acts to a state.[48] While it did not expound on the exact meaning of this requirement, it should, like that of the Iran Claims Tribunal, be understood as imposing a fairly high standard of proof. Nevertheless, "clear evidence" is not to be equated with the demanding criminal law "beyond a reasonable doubt" standard of proof.[49] Absolute certainty, or at least the elimination of all possible alternatives, is not required.

Illustrating this point with a recent example, the Mandiant report indicated that the Chinese PLA's Unit 61398 (also known as Comment Crew or APT1) acted with the full knowledge and cooperation of the Chinese government.[50] Some have challenged this assertion,[51] but so long as the victim states acted with reasonable certainty based on clear evidence that China is behind the operations, they would have been within the bounds of the law in responding through demands for cessation, claims of reparations, or countermeasures. The same analysis applies to Syria's most prominent hacker group, the Syrian Electronic Army. Although it insists that it operates independently of the Assad regime, there

on State Responsibility (para. 9 of chapeau to Chapter II).

46 Oil Platforms (Iran v. US), 2003 I.C.J. 161 (Nov. 6) [hereinafter Oil Platforms], Separate Opinion of Judge Higgins, para. 33.

47 Articles on State Responsibility, art. 51.

48 Nicaragua, para. 109.

49 See, e.g., Michael N. Schmitt, "Counter-Terrorism and the Use of Force in International Law," *Marshall Center Papers*, no. 5 (2002): 69.

50 *APT1: Exposing One of China's Cyber Espionage Units* (Mandiant, 2013), 59, accessed January 31, 2014, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

51 Jeffrey Carr, "Mandiant APT1 Report Has Critical Analytic Flaws," *Digital Dao* (blog), February 19, 2013, http://jeffreycarr.blogspot.com/2013/02/mandiant-apt1-report-has-critical.html.

are indications to the contrary.[52] Injured states would be entitled to respond against Syria itself if sufficiently reliable and substantive evidence emerged that the relationship with the regime met the thresholds described above.

The prevailing view is that the law of state responsibility does not allow the taking of forceful countermeasures.[53] Accordingly, a state generally may not respond with cyber or kinetic operations that rise to the level of a use of force against a state instructing or effectively controlling a proxy's cyber operation. There is one important exception — self-defense.

The Law of Self-Defense

A right enshrined in Article 51 of the UN Charter, and reflective of customary international law, is that states are allowed to exercise their "inherent right of individual or collective self-defence if an armed attack occurs." In an international legal system in which use of force is prohibited, self-defense is one of the two generally accepted grounds that permit a state to resort to force, the other being authorization or mandate from the UN Security Council.[54]

A cyber operation is deemed to constitute an "armed attack" if its scale and effects are grave. Significant injury, death, physical damage, or physical destruction qualify.[55] In the absence of state practice and *opinio juris*, the case of non-destructive, albeit highly disruptive, cyber operations such as those interfering with critical infrastructure, is unsettled. During the *Tallinn Manual* deliberations, members of the International Group of Experts took different positions on this issue. While some insisted on the requirement for physical injury or damage, others focused on the severity of the non-destructive consequences and were willing to characterize non-destructive but otherwise catastrophic cyber operations as armed attacks.[56]

A key issue concerns Article 51's relation to Article 2(4). In the *Tallinn Manual*, the majority of the International Group of Experts took the position that a cyber armed attack is always a cyber "use of force" in the Article 2(4) sense, but the reverse is not the case. Rather, cyber "armed attacks" are those cyber uses of force that have particularly serious consequences.[57] In *Nicaragua*, the International Court of Justice adopted an identical position when it noted the need to "distinguish the most grave forms of the use of force (those constituting an armed attack) from other less

52 See, e.g., Nicole Perlroth, "Hunting for Syrian Hackers' Chain of Command," *New York Times*, May 17, 2013, http://www.nytimes.com/2013/05/18/technology/financial-times-site-is-hacked.html.

53 Articles on State Responsibility, art. 50(1)(a); cf. Oil Platforms, Separate Opinion of Judge Simma, para. 13.

54 U.N. Charter, arts. 39, 42.

55 Tallinn Manual, para. 6 of commentary to Rule 13.

56 Ibid., para. 9 of commentary to Rule 13.

57 Ibid., para. 6 of commentary to Rule 13.

grave forms."[58] The distinction has particular relevance in the case of proxies. To the extent a proxy conducted cyber use of force is attributable to a state, Article 2(4) prohibits the injured state from responding with its own forceful action against the responsible state until the consequences cross the armed attack threshold. Should it not, the state may only engage in retorsion, demand cessation, seek reparations, or launch countermeasures. The United States has adopted a minority view on the matter. It suggests there is no "gap" between a use of force and an armed attack. Every use of force is an armed attack in the absence of either a self-defense justification or enabling Security Council resolution.[59] Therefore, once a non-state actor conducts a cyber operation at the use of force level, the victim state may respond forcefully.

An on-going debate in international law circles also surrounds the applicability of Article 51's right of self-defense to hostile actions by non-state actors; the debate equally resonates with respect to cyber attacks conducted by non-state actors. Views have crystallized around two schools of thought. The first suggests that force is only permitted under Article 51 when the non-state group's operations are attributable to a state. Proponents point to two controversial International Court of Justice cases in which the Court appeared to take this position.[60] Absent attribution, they argue, only responses within the law enforcement paradigm are permissible.

The decisions were criticized even by key judges of the Court who, correctly in the view of the authors, noted that the plain text of Article 51 contains no limitation of armed attacks to those conducted or attributable to states and that state practice in the aftermath of the 9/11 attacks augurs towards the opposite conclusion.[61] The United States unambiguously agrees with this position,[62]

58 Nicaragua, para. 191.

59 A former (then sitting) State Department Legal Adviser articulated the US position in Harold H. Koh, "International Law in Cyberspace," Address at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, Maryland on September 18, 2012, reprinted in Harold Hongju Koh, "International Law in Cyberspace," *Harvard International Law Journal Online* 54, (2012): 1-12. The Koh address and the Tallinn Manual are compared in Michael N. Schmitt, "The Koh Speech and the Tallinn Manual Juxtaposed," *Harvard International Law Journal Online* 54, (2012): 13-37.

60 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, para. 139 (July 9) [hereinafter Wall]; Armed Activities in the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, paras. 146-47 (Dec. 19) [hereinafter Congo].

61 Wall, Separate Opinion of Judge Higgins, para. 33; Wall, Separate Opinion of Judge Kooijmans, para. 35; Wall, Declaration of Judge Buergenthal, para. 6; Congo, Separate Opinion of Judge Simma, para. 11.

62 *Lawfulness of a Lethal Operation Directed Against a US Citizen Who is a Senior Operational Leader of Al-Qa'ida or an Associated Force* (Department of Justice White Paper), 2, accessed January 31, 2014, http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf. See also Harold H. Koh, Legal Adviser, US Department of State, "The Obama Administration and International Law," Address Before the American Society of International Law on March 25, 2010, accessed

as did the majority of the *Tallinn Manual* International Group of Experts.[63] This debate resonates in the cyber context because if the Court's position is correct, states subjected to injurious or destructive cyber attacks by non-State actors will be severely limited in their response options. Therefore, they are unlikely to countenance such a restriction.

The essential question for the purposes of this article is: When do a non-state group's cyber operations, generating consequences at the level of armed attack, involve sufficient attributability that the victim state can use kinetic or cyber operations at the use of force level against another state (as well as the group itself)? In this regard, the normative *locus classicus* is the International Court of Justice's treatment of the subject in its *Nicaragua* judgment when assessing US support to the Contra guerrillas.

> *[I]t may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to" (inter alia) an actual armed attack conducted by regular forces, "or its substantial involvement therein". This description, contained in [...] the Definition of Aggression annexed to General Assembly resolution 3314 (XXIX), may be taken to reflect customary international law.*
>
> *The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States.*[64]

Applied to cyber proxies, the pronouncement leads to certain conclusions. First, the standards track those developed

January 31, 2014, http://www.state.gov/s/l/releases/remarks/139119.htm.

63 Tallinn Manual, para. 17 of commentary to Rule 13.

64 Nicaragua, para. 195.

above in the context of state responsibility. A non-state group that is "sent" by a state to launch cyber attacks against another state or one that is acting "on its behalf" is essentially operating on its instructions or is under its effective control. The "substantial involvement" reference can best be understood as joint

> ***"States must clearly articulate their position on the matter whenever it can be established that a state has resorted to a proxy to conduct harmful cyber operations."***

operations. Once these preconditions are met, attribution results. But the right to respond in self-defense will only mature at the point that the non-state group's cyber activities amount to an armed attack. There is no difference between the requisite consequential threshold applying to its activities and those of a state's armed forces in this regard. Finally, the text makes it clear that although providing cyber weapons to the group or offering other support such as enabling it to make use of the state's cyber infrastructure to conduct its operations is wrongful, such activities do not endow the injured state with the right to use force against that state (although it might be able to use force against the group itself).

International Humanitarian Law

International humanitarian law (also known as the law of armed conflict) regulates the conduct of armed conflict. It distinguishes between two genres of armed conflict — an "international armed conflict" between two or more states and a "non-international armed conflict" between a state and an organized armed group, or between such groups.[65] Non-state actors may play a crucial role in both. The issue of attribution looms largest with respect to whether state support creates an international armed conflict between the two states.

The legal consequences of this form of attribution differ from those discussed above. Attribution in this context serves an initiating or transformative function with respect to the conflict itself. This occurs in one of two ways. First, certain support of a non-state group initiates an international armed conflict where no armed conflict at all was previously underway. Second, support by an external

65 Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, arts. 2 & 3, Aug. 12, 1949, 6 UST. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, arts. 2 & 3, Aug. 12, 1949, 6 UST. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, arts. 2 & 3, Aug. 12, 1949, 6 UST. 3316, 75 U.N.T.S. 135; Convention Relative to the Protection of Civilian Persons in Time of War, arts. 2 & 3, Aug. 12, 1949, 6 UST. 3516, 75 U.N.T.S. 287.

state can "internationalize" an on-going non-international armed conflict such the states concerned are now in an international armed conflict. The legal significance of these dynamics is that IHL rules, and related bodies of law such as the law of neutrality, now apply as between the States. Resultantly, members of the armed forces of the sponsoring state and any of its civilians who directly participate in the hostilities become targetable. So too do any "military objectives" in the State.[66] Therefore, all the sponsoring state's cyber infrastructure that is military in character or used for military purposes qualifies as a lawful target even if it is geographically very remote from the on-going hostilities between the other state and the non-state group.[67]

In determining whether a state's support to a non-state actor either initiates an armed conflict between the states concerned or internationalizes a non-international armed conflict, it is necessary to distinguish between support to organized armed groups and that to a relatively unorganized group or to an individual engaged in cyber operations. With regard to the former, the requisite degree of control over the organized armed group for the purposes of finding an international armed conflict differs from that employed in order to establish state responsibility.[68] Whereas a state's responsibility attaches if the state instructs or has "effective control" over the non-state actor, an armed conflict is initiated or internationalized once the sponsoring state exercises "overall control" over an organized armed group.[69] In *Tadić*, the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia found that "the mere financing and equipping of such forces" was insufficient, whereas "participation in the planning and supervision of military operations" qualified.[70] In *Lubanga,* the International Criminal Court confirmed that "a role in organising, co-ordinating, or planning the military actions of the military group" internationalizes a non-international armed conflict.[71] In contradistinction to the attribution standards of state responsibility, no requirement exists that the non-state group be acting pursuant to specific orders or instructions regarding a particular operation.

By this standard, a state which identifies cyber targets for an organized armed group, provides it essential intelligence necessary to launch destructive attacks, or

66 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 51, 52, June 8, 1977, 1125 U.N.T.S. 3; *Customary International Humanitarian Law,* eds. Jean-Marie Henckaerts and Louise Doswald-Beck (New York: Cambridge University Press, 2005): Rules 1, 6, 7.

67 Tallinn Manual, Rule 38 and accompanying commentary.

68 Genocide, para. 405.

69 Prosecutor v. Tadi , Case No. IT-94-1-A, Appeals Chamber Judgment, para. 145 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) [hereinafter Tadi].

70 Ibid.

71 Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, para. 211 (ICC Jan. 29, 2007).

participates in the planning of the group's military cyber operations becomes a party to an international armed conflict with the target state. In a more general sense, once a state exercises enough control over the group to direct it to mount a broad campaign of cyber attacks, that state enjoys overall control. By the same token, if the state has the power to terminate a military cyber campaign or instruct the group to refrain from attacking a particular category of cyber targets, its level of control qualifies as overall control. But neither providing malware or hardware nor providing the group with financing for its cyber operations are enough.

Support to an organized armed group must be distinguished from that to a single private individual or a group that is not well organized, as in the case of an *ad hoc* group that communicates on-line but has no command structure and does not operate collaboratively. Here, the law requires that the state exercise much greater control over those conducting cyber operations before an international armed conflict results between the two states. The *Tadic* Appeals Chamber cited the example of "specific instructions or directives aimed at the commission of specific acts."[72] For instance, if a state instructs a highly capable small collection of hackers (or an individual hacker) to conduct a lethal or destructive attack against another state's cyber infrastructure, an international armed conflict results.

It must be cautioned that there is insufficient state practice accompanied by *opinio juris* to answer the question of whether cyber operations that result in no physical damage or injuries can initiate an international armed conflict (clearly those that do suffice) where no armed conflict was previously underway.[73] It is likely that in making that assessment, states will take into account factors such as the severity of the cyber operation's consequences, whether its target is of a military nature or not, and the duration of the cyber operation.[74]

Conclusion

That states will continue to work through non-state actors to achieve national security and foreign policy objectives is inevitable. In cyberspace, this tendency will certainly grow, for such operations afford states a degree of anonymity and detachment from the non-state operations that serve useful political and legal ends. In particular, the relatively high levels of support that are required before a state can be held responsible for the activities of non-state groups or individuals, as distinct from their own responsibility for being involved, creates a normative safe zone for them.

72 Tadi , para. 132. See also paras. 137, 141.

73 Michael N. Schmitt, "Classification of Cyber Conflict," *International Law Studies* 89 (2013): 241. See also Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," *International Review of the Red Cross* 94, no. 886 (2012): 549.

74 Droege, "Get Off My Cloud," 547.

This does not mean that states may turn to non-state actors with impunity to conduct cyber operations in their stead against other states. Pursuant to the law of state responsibility, they may face the prospect of reparations or countermeasures when they either instruct the actors to mount the operations or exercise effective control over them. Should such operations generate consequences crossing the armed attack threshold, the state may find itself the target of forceful cyber or kinetic responses pursuant to the law of individual or collective self-defense. And if the state either instructs non-state actors to launch physically destructive or lethal operations against another state, or exercises overall control over an organized armed group, it will find itself "at war" with the target state.

As should be apparent, therefore, states contemplating a relationship with non-state actors involved in cyber operations against another state must tread very lightly. To the extent they engage in such operations, they weaken the international legal architecture for assessing responsibility and imposing accountability with respect to harmful cyber operations. This is because it is always necessary to look to state practice when interpreting legal norms that lack absolute clarity. By using non-state actors, states effectively help hold the legal door open for other states to do likewise.

For the same reasons, states must clearly articulate their position on the matter whenever it can be established that a state has resorted to a proxy to conduct harmful cyber operations. Silence will typically be interpreted as acquiescence, although that is technically a questionable conclusion as a matter of law. Only by objecting to such use based on strict application of the law of state responsibility's rules on attribution can states hold the line against actions that weaken the extant norms.

Finally, there is little prospect for establishment of a treaty regime to deal with the use of proxy cyber actors. States that turn to them will be hesitant to embrace such a regime and, absent their consent, treaties do not bind states. Therefore, the reality is that states can only shape understanding of the current law through their practice. Unfortunately, the vector of that state practice is presently uncertain.

Professor Michael N. Schmitt is Director of the Stockton Center for the Study of International Law at the United States Naval War College. He is also Professor of Public International Law at the University of Exeter (UK), Honorary Professor of International Humanitarian Law at Durham University (UK), and Senior Fellow at the NATO Cyber Defence Centre of Excellence.

Ms. Liis Vihul works as a legal analyst in the Law and Policy Branch at the NATO Cooperative Cyber Defence Centre of Excellence and has been with the organization since 2008. She holds an MA in law from the University of Tartu, and an MSc in information security from the University of London.

WWW.FLETCHERSECURITY.ORG

@FLETCHERSECREV