THE YALE LAW JOURNAL FORUM
JUNE 22, 2015

In Defense of Due Diligence in Cyberspace

Michael N. Schmitt

INTRODUCTION

Recent events such as the attack on Sony by North Korea and revelations that Russians hacked President Obama's e-mail have drawn attention to the dilemma of harmful transborder state and non-state cyber operations against government and private cyber infrastructure.[1] Academics and practitioners have analyzed whether cyber operations violate international law, especially the sovereignty of the state where they manifest,[2] and when they can be attributed to a state pursuant to the law of state responsibility.[3] But little attention has been paid to a state's legal responsibilities when cyber infrastructure located on its territory is used by another state—or by non-state actors, such as hacker groups, individual hacktivists, organized armed groups, or terrorists—to mount the operations.[4] This question has, for reasons to be explained, become ripe for serious consideration.

1. Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014, 9:29 AM), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea [http://perma.cc/NE6S-NMH8]; Michael S. Schmidt & David E. Sanger, *Russian Hacker's Read Obama's Unclassified Emails, Officials Say*, N.Y. TIMES, Apr. 26, 2015, http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html [http://perma.cc/CDA2-5C52]. While Chinese hackers tend to target commercial entities, their Russian counterparts often have political aims.

2. Wolff Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123 (2013).

3. Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, 1 FLETCHER SECURITY REV., no. 2, at 55 (2014). For academic treatment of state responsibility in general, see JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART (2013).

4. A notable exception with respect to due diligence generally is INT'L LAW ASS., ILA STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW: FIRST REPORT, (Mar. 7, 2014) [hereinafter ILA REPORT], http://www.ila-hq.org/download.cfm/docid/8AC4DFA1-4AB6-4687-A265FF9C0137A699 [http://perma.cc/WX88-SBDX].

Although states are now examining how current international law governs cyberspace in fora like the U.N. Group of Governmental Experts (GGE), progress is agonizingly slow.[5] They are on the horns of a dilemma. On the one hand, if states build "normative firewalls" by adopting interpretations of the existing law that restrict cyber operations, they will paradoxically also limit their own freedom of action in cyberspace. Alternatively, any interpretive crystallization that safeguards the margin of discretion enjoyed by state's vis-à-vis cyber activities necessarily leaves their cyber systems at risk. Since states accordingly find themselves conflicted when trying to make legal-policy decisions regarding cyber norms, virtually all in-depth work in the field has emerged from the academy.[6] This is an unfortunate reality with deleterious consequences for international law making.

The dilemma is especially evident with respect to "due diligence," the obligation of states to take measures to ensure their territories are not used to the detriment of other states. While states may resist application of the norm to cyber activities because of the burden they fear the principle may impose, they equally will want to ensure that other states take every feasible step to put an end to harmful cyber activities launched from—or through—their own territory. They are struggling to decide how best to approach the matter.

This Essay considers applying the principle of due diligence in the cyber context. It questions the sensibility of nascent state opposition to its application by asking whether the opportunity costs of rejecting such application outweigh any burdens avoided. Concluding that they do, the Essay highlights the norm's utility when states find themselves facing harmful cyber operations conducted by non-state actors or other originators of the operations who cannot reliably be identified.

I. THE *TALLINN MANUAL* PROCESS AND EARLY DISCUSSIONS OF DUE DILIGENCE IN INTERNATIONAL CYBER LAW

As noted, academic discourse has dominated consideration of how international law applies in cyberspace. The most robust such examination commenced in 2009 when the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) invited twenty international law experts, the so-called International Group of Experts (IGE), to identify those elements of the existing

5. S*ee, e.g.*, U.N. Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/68/98 (June 24, 2013) [hereinafter 2013 GGE Report]; U.N. Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/65/201 (July 30, 2010). The GGE currently consists of representatives from twenty states.

6. *E.g.*, Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 TEX. INT'L L.J. 189 (2015).

international law that pertain to cyber activities and interpret them in light of cyberspace's unique characteristics. The project concluded in early 2013 with publication of the *Tallinn Manual on the International Law of Cyber Warfare*, a restatement of law consisting of ninety-five "black letter" rules and accompanying commentary.[7]

The *Tallinn Manual* concentrates on the *jus ad bellum*, the law that addresses when states may resort to force as an instrument of their national policy,[8] and the *jus in bello*, international humanitarian law, which sets limits on how hostilities may be conducted during armed conflicts.[9] In other words, it focuses on laws for wartime, not peacetime. However, the manual briefly addresses several key aspects of peacetime law to signal that not all cyber incidents are properly analyzed in the context of use of force norms.

Due diligence is dealt with in a single rule accompanied by brief commentary. That rule provides that "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States."[10] The experts unanimously agreed that states shoulder a due diligence obligation with respect to both government and private cyber infrastructure on, and cyber activities emanating from, their territory.[11] They likewise agreed that if a state fails to meet its due diligence obligation, a victim state may resort, when appropriate, to legal remedies such as countermeasures or self-defense.[12]

The IGE could not, however, achieve consensus on the exact parameters of the obligation. For instance, although the experts concurred that the obligation attaches once harmful cyber activities are underway, there was no agreement as to whether the due diligence obligation applies when a state knows that such

---

7. Rules required unanimous agreement, whereas commentary set forth all reasonable interpretations thereof.

8. U.N. Charter art. 2(4). For a discussion of the use of force in the cyber context, see INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 45-52 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL], which provides Rules 10-12 and accompanying commentary.

9. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field arts. 2 & 3, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea arts. 2 & 3, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention (III) Relative to the Treatment of Prisoners of War arts. 2 & 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Convention (IV) Relative to the Protection of Civilian Persons in Time of War arts. 2 & 3, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287. For a discussion of qualification of cyber operations as armed conflict, see TALLINN MANUAL, *supra* note 8 (Rules 22 & 23 and accompanying commentary); and Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INT'L L. STUD. 233 (2013).

10. TALLINN MANUAL, *supra* note 8, at 27 (Rule 5).

11. *Id.* at 26 cmt. 1.

12. *Id.* at 29 cmt. 13.

activities will be launched but they have not yet materialized.[13] Nor did they agree on whether a state must take preventive measures to ensure the cyber hygiene of the infrastructure on its territory or whether states should be required to monitor for malicious activity that might be directed at other states.[14] And although all the experts were of the view that the territorial state must have knowledge of the harmful activity concerned, they also failed to reach accord as to whether constructive knowledge suffices for establishing a breach of the obligation.[15]

The CCD COE is currently sponsoring a follow-on project with a new International Group of Experts—"Tallinn 2.0"—that will fully develop the peacetime law of cyber operations.[16] Among the topics the experts are examining is due diligence, this time in a more systematic and in-depth fashion than was the case with the *Tallinn Manual* process. The Tallinn 2.0 IGE will formally meet twice in 2015, with project completion scheduled for mid-2016.

In preparation for those sessions, the project leaders explained their initial approach on due diligence during a May 2015 meeting of legal advisers from thirty-five states that was organized jointly by the CCD COE and the Dutch Ministry of Foreign Affairs.[17] Although held under the Chatham House Rule, it can be reported that the team encountered some push back from at least one key state with respect to a due diligence obligation in cyberspace. This reaction raises two questions: whether states should be tentative about applying the principle of due diligence, and whether states have fully considered the consequences of failing to apply it. In the author's opinion, the answer to both questions is "no."

II. THE OPPOSITION TO DUE DILIGENCE IN INTERNATIONAL CYBER LAW

Some states are hesitant about applying the principle of due diligence to cyber activities because of the corresponding obligations that it would impose on them. Due diligence derives from the principle of sovereignty.[18] To the

13. *Id.* at 27 cmts. 6-7.

14. *Id.*

15. *Id.* at 28 cmts. 10-11.

16. For a description, see *Tallinn Manual*, NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE, http://ccdcoe.org/research.html [https://perma.cc/DV6W-SBL5].

17. Paul Rosenzweig, *Tallinn 2.0*, LAWFARE (Apr. 27, 2015), http://www.lawfareblog.com/tallinn-20 [http://perma.cc/898S-8SE9]. The author briefed the NATO North Atlantic Council and led the group presenting to the legal advisers.

18. A corollary of sovereignty is the duty "to protect within the territory the rights of other states, in particular their right to integrity and inviolability in peace and in war . . . ." Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928).

extent that a state enjoys the right to exercise sovereignty over objects and activities within its territory, it necessarily shoulders corresponding legal obligations. In the *Trail Smelter* arbitration, an international arbitral tribunal ruled in 1941 that a state "owes at all times a duty to protect other states against injurious acts by individuals from within their jurisdiction."[19] Eight years later, the International Court of Justice addressed the duty in its first case, *Corfu Channel*, when it stated, "it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[20] The *Tallinn Manual* restated the law as follows:

> States are required under international law to take appropriate steps to protect those rights. This obligation applies not only to criminal acts harmful to other States, but also, for example, to activities that inflict serious damage, or have the potential to inflict such damage, on persons and objects protected by the territorial sovereignty of the target State.[21]

It is incontrovertible that states enjoy sovereignty over cyber infrastructure and activities located on their territory.[22] The original IGE therefore concluded that the general legal duty of due diligence encompasses taking appropriate remedial action when non-state actors launch harmful cyber operations from that territory, a position that seems to have been accepted by at least Russia.[23] For the experts, the duty would similarly apply to situations in which a third state or a non-state actor operating from outside the state's territory takes control of cyber infrastructure on its territory to mount operations against another state.

But whether transit states—states through which the operations merely travel—bear a due diligence obligation is less clear. The IGE was divided on the issue, with some experts taking the position that if the transit state knows of the operation and is in a position to terminate it, it must do so. Others hesitated to extend the obligation to transit states, arguing that customary law

---

19. Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941).

20. Corfu Channel (UK v. Alb.), Judgment, 1949 I.C.J. 4, 22 (April 9); *see also* Memorandum, U.N. Secretary-General, Survey of International Law in Relation to the Work of Codification of the International Law Commission: Preparatory Work Within the Purview of Article 18, Paragraph 1, of the International Law Commission 57, U.N. Doc. A/CN.4/1/Rev.1 (Feb. 1, 1949).

21. TALLINN MANUAL, *supra* note 8, at 26 cmt. 3.

22. *Id.* at 15-18 (Rule 1 and accompanying commentary).

23. Andrey Krutskikh & Anatoly Streltsov, *International Law and the Problem of International Information Security*, 60 INT'L AFF. 64, 70 (2014). Krutskikh is the Russian representative to the U.N. Group of Governmental Experts and an Ambassador-at-Large of Russian Ministry of Foreign Affairs.

had not yet crystallized beyond activities launched from a state's territory and that it would be technically impossible for the transit state to comply with any this due diligence obligation. However, capabilities are apparently improving in the latter regard; should identifying and terminating transit of malware across cyber infrastructure on a state's territory become feasible, there would seemingly be no reason to excuse that state from the obligation of due diligence.

States that are circumspect about application of the due diligence principle to cyber activities generally cite practical and policy concerns regarding its implementation. The legal basis for their disquiet is less clear. For instance, in one of its few substantive pronouncements on legal matters, the GGE, which includes, *inter alia*, Russia, China, the United States, and the United Kingdom, concluded that "[i]nternational law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible [information and communications technology] environment."[24] Yet, when turning to due diligence, the GGE punted, framing the principle in hortatory, rather than obligatory, terms: "States *should* seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs."[25] A degree of indecision was again apparent, as mentioned above, during the presentation of the Tallinn 2.0 approach on the subject to states. In neither case was a principled and detailed legal argument against application put forth.

Perhaps the best legal basis for objection is that the due diligence principle's firmest grounding is in the environmental realm,[26] as exemplified by the well-known *Trail Smelter* arbitration,[27] and that insufficient state practice and *opinio juris* exist to extend the principle to other contexts. But in international law, it is unnecessary to identify a distinct reason to apply a general principle in a particular context. On the contrary, since it is a general principle, the presumption is that the principle applies unless state practice or *opino juris* excludes it.[28]

---

24. 2013 GGE Report, *supra* note 5, ¶ 19.

25. *Id*. at 23 (emphasis added).

26. U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, princ. 2, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I), annex I (Aug. 12, 1992).

27. Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941).

28. In this regard, also recall the general tendency against finding a situation to be *non liquet*. North Sea Continental Shelf (F.R.G./Den., F.R.G./Neth.), Judgment, 1969 I.C.J. 3, ¶¶ 83, 88-91 (Feb. 20) (filling a presumed gap through application of equity). *But see* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 105 (July 8) (refusing to opine in situations in which the survival of the state is at stake); Prosper Weil, *"The Court Cannot Conclude Definitively . . ."* Non Liquet *Revisited*, 36 COLUM. J. TRANSNAT'L L. 109 (1998).

Reticence to embrace the principle as applicable to cyberspace is nevertheless understandable, for cyber infrastructure in some states is frequently used for launching or otherwise facilitating harmful cyber operations abroad without any State involvement that might result in legal attribution to the state.[29] Moreover, difficulties in factual attribution can hinder a state's ability to take steps to terminate the operations, as can the practical difficulties of terminating them. And while domestic law obstacles do not relieve a state of its international law obligations, as a policy matter they too can represent a hurdle for a state trying to control cyber activities on its territory.

The concern is perhaps most acute for highly "connected" states, as they have the highest malware infection rates.[30] Because of this reality, such states are extremely vulnerable to having cyber infrastructure on their territory taken over by malicious actors, converted into botnets, and used for attacks against other states. It is these states that will bear the heaviest burden of due diligence.

However, such challenges do not speak to the underlying legal obligation, but rather to the feasibility and reasonableness of carrying out that obligation. Numerous aspects of the due diligence principle should limit these states' concerns.[31]

First, if taking measures to counteract harmful cyber activities directed abroad is technically impractical, the state that fails to do so is not in breach of its due diligence obligation; the diligence that is due under the legal standard cannot exceed the state's capabilities. This scenario may well arise when, for instance, a distributed denial of service attack is mounted from widely dispersed bots of a botnet.[32] Even if the state succeeds in terminating use of many of the bots, the attack can often continue apace so long as significant numbers of them remain in the bot herder's control. The technical difficulty of reliable factual attribution—of finding the culprit—further limits a state's

29. On attribution in the law of state responsibility, see generally Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, pt. 1, ch. II, U.N. Doc. A/RES/56/83 (Jan. 28, 2002) [hereinafter Articles on State Responsibility].

30. According to ESG MalwareTracker, for example, the states with the highest malware infection rates at the time of this writing are the United States, France, Italy and Germany. *ESG MalwareTracker*, ENIGMA SOFTWARE, http://www.enigmasoftware.com/malware-research/malwaretracker [http://perma.cc/4N8W-8XNF].

31. *See, e.g.*, Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, Case No. 17, Advisory Opinion of Feb. 1, 2011, ¶ 117, http://www.itlos.org/fileadmin/itlos/documents/cases/case_no_17/17_adv_op_010211_en.pdf [http://perma.cc/8Z5Y-KPAC]; ILA REPORT, *supra* note 4, at 26-27.

32. A distributed denial of service attack involves taking control of multiple, sometimes thousands, of computers (known as bots or zombies) and using them together (the botnet) to overwhelm the target system with communications, such that it no longer functions as intended.

ability to act. But as noted in the *Tallinn Manual*, a breach only occurs when the state concerned "fails to take reasonably feasible measures to terminate the conduct."[33]

Furthermore, as highlighted by the International Law Association's Study Group on due-diligence obligations:

> "[t]he due diligence standard . . . varies in many contexts on the basis of common but differentiated responsibilities. It is well-established that developing States may not be able to control the activities in their territory in a similar manner to developed States, and that this will effect [sic] the evaluation of whether they have breached their due diligence obligation."[34]

Given that the obligation is highly sensitive to the capabilities of the states concerned, states need not fear that they will be expected to bear a burden that is excessive relative to their proficiency and technical wherewithal.

Second, if the burden on the territorial state in taking remedial actions is so onerous as to be unreasonable under the circumstances, inaction will not constitute a breach. In gauging reasonableness, "[t]he nature, scale, and scope of the (potential) harm to both States must be assessed."[35] It would be incongruent to impose the obligation in situations in which the burdens levied on the territorial state far outweigh the harm being imposed on the target state. For example, a state may be able to terminate the harmful operation by taking the network from which it is being launched offline, but doing so may also negatively affect its own activities that are dependent on the network. While the appropriate balance between relative harm may be ambiguous as a matter of international law, and although states may have to suffer some disruption, a state clearly need not act when the burden becomes disproportionately heavy.

Third, the due diligence obligation only indisputably applies to ongoing cyber activities that are generating serious adverse effects in another country—although they need not be physically destructive or injurious.[36] As noted, all the IGE could agree on was that the obligation attached to ongoing activities and that it expires once the offending cyber operation is complete (at least if it is unlikely to be repeated). There appears to be an emerging consensus among scholars and state legal advisers against the existence of obligations either to monitor cyber activities on one's territory or to prevent malicious use of cyber infrastructure located within one's borders. The obligation of due diligence attaches only once the offending cyber activity comes to the state's attention,

---

33. TALLINN MANUAL, *supra* note 8, at 27 cmt. 6.

34. ILA REPORT, *supra* note 4, at 27.

35. TALLINN MANUAL, *supra* note 8, at 27 cmt. 4.

36. *Id*. at 27 cmts. 5-6.

for instance because the target state notifies it of the operations or because they have been picked up by the territorial State's Computer Emergency Response Team (CERT). Furthermore, although the precise threshold of harm at which the duty arises is unclear in law,[37] there has been no suggestion from any quarter that the duty extends to mere irritation or inconvenience, such as defacement and temporary minor denials of service. Rather, harm must rise to such a level that it becomes a legitimate concern in inter-state relations and, thus, an appropriate subject of international law rights and obligations.

III. THE CONSEQUENCES OF OPPOSING THE DUE DILIGENCE OBLIGATION

According to the 2015 Department of Defense's (DOD) Cyber Strategy, "during heightened tensions or outright hostilities, DOD must be able to provide the President with a wide range of options for managing conflict escalation."[38] Discarding lawful and operationally viable options for doing so would be an imprudent step for any state. Those presently evaluating the application of the due diligence principle to cyber activities would be well-advised to reflect carefully on what rejecting it would take off the table.

When a state conducts a harmful cyber operation, the operation will often amount to an "internationally wrongful act"[39] that opens the door to countermeasures by the so-called "injured" state. Under the law of state responsibility, countermeasures are acts that would be unlawful but for an underlying wrongful act by another state (the "responsible state" in state responsibility parlance) that breaches an obligation owed the injured state.[40] In the cyber context, therefore, an injured state may respond to a responsible state's unlawful cyber operations by means that would normally be prohibited, like conducting operations that would otherwise violate the responsible state's sovereignty because they affect the functionality of its government cyber infrastructure.[41]

---

37. Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1911, 1963 (Arb. Trib. 1941).

38. *The DoD Cyber Strategy*, DEP'T OF DEF (Apr. 2015), http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [http://perma.cc/9223-22Y9].

39. An international wrongful act is one that (1) breaches an obligation one state owes another under international law, and (2) is attributable to the state pursuant to the law of state responsibility. *See* Articles on State Responsibility, *supra* note 29, at arts. 1-3, 12.

40. *Id*. at arts. 21, 49; *see also* TALLINN MANUAL, *supra* note 8, at 36-41 (Rule 9 and accompanying commentary); Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014).

41. For the original Tallinn Manual discussion of sovereignty, see TALLINN MANUAL, *supra* note 8, at 15-18, which provides Rule 1 and accompanying commentary. See especially comment 6.

The countermeasures need not be in kind: cyber countermeasures may be used to respond to non-cyber internationally wrongful acts, and vice versa. Nor must countermeasures involve the same legal obligation that was initially breached by the responsible state.[42] As an example, a state targeted with cyber operations may decide to respond by suspending the right of the responsible state's ships to transit through its territorial sea under the innocent passage regime.[43] Moreover, depending on the nature of the wrongful act, countermeasures may be directed not only at government entities, but also at private ones. For instance, if a state launches hostile cyber operations at private companies on another state's territory, as with the Sony hack, thereby violating that state's sovereignty, the injured state may respond by mounting responsive cyber operations against private companies in the responsible state.

Countermeasures can prove a robust and flexible tool for returning a situation to one of lawfulness, their only permissible purpose under the law of state responsibility.[44] Yet there are significant procedural and substantive restrictions placed on the taking of countermeasures.[45] They are unavailable as a matter of law as a direct response to cyber operations by non-state actors unless the operations are legally attributable to a state, as would be the case when a state directs, controls, or adopts the cyber operations of a non-state actor.[46] The limitation of countermeasures to acts by or attributable to states is of particular significance given the fact that today non-state actors conduct the vast majority of harmful cyber operations.

In light of these constraints, the plea of necessity may offer states facing harmful non-state cyber operations some relief. Taking measures based on necessity is permissible when they are the sole means by which a state can "safeguard an essential interest against a grave and imminent peril."[47] Like

---

42. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 285-86 (2002).

43. United Nations Convention on the Law of the Sea arts. 17 & 19, Dec. 10, 1982, 1833 U.N.T.S. 397. Although the United States is not a party to the Convention, it recognizes the provisions on innocent passage as reflective of customary international law. DEP'T OF THE NAVY, THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS § 2.5.2.1 (July 2007).

44. Articles on State Responsibility, *supra* note 29, at art. 49(1).

45. *Id*. at arts. 49-53.

46. *Id.* On attribution of non-state actor actions, see *id.* at art. 8; and Schmitt & Vihul, *supra* note 3, at 61-66.

47. Articles on State Responsibility, *supra* note 29, at art. 25(1). Necessity (or phraseology clearly referring to necessity) has been cited in many contexts. *See, e.g.*, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 140 (July 9) (security); Legality of the Threat or Use of Nuclear Weapons, *supra* note 28, ¶ 105 (survival of the state); Rainbow Warrior (N.Z./Fr.), 20 R.I.A.A. 217, 254-63 (Arb. Trib. 1990). For academic treatment of the subject, see Robert D. Sloan, *On the Use and Abuse of Necessity in the Law of State Responsibility*, 106 AM. J. INT'L L. 447 (2012).

countermeasures, the plea may be resorted to in response to a qualifying situation irrespective of whether the interest concerned is private or governmental.

The defining feature of the plea of necessity in the cyber context, however, is that states may resort to the plea as the basis for a response against non-state actors whose conduct may not be attributable to another state. Necessity may also provide a legal basis for responding to cyber operations in which the actual author of the operation is unknown or uncertain, as when the origin of the attack is spoofed. The state need only locate the technological source of the harmful operation and assess the consequences of its own response—factual and legal attribution is not a precondition to action. Responses are permissible even when they amount to an internationally wrongful act, such as a violation of the sovereignty of a state that is completely uninvolved in the underlying harmful cyber operations, so long as the response does not seriously impair an essential interest of that state. Consider the case of a state that is doing everything feasible to stop harmful cyber operations from its territory. Despite its best efforts, the operations have shut down critical infrastructure in another state. The latter state would be entitled to take necessary measures to put an end to the operations even if doing so affected various nonessential cyber activities in the former. As illustrated by this example, the plea of necessity serves as a failsafe for a state facing severe cyber operations from outside its borders, especially when they cannot be attributed to another state.

But the high threshold for invoking the plea limits its utility. First, an essential interest must be involved. Critical cyber infrastructure (a disputed term in itself) likely qualifies, but it is unclear what other entities and activities are properly styled as "essential." Second, the threat to that essential interest must be "grave." Few cyber operations cause harm at this level—although if terrorists begin to employ cyber operations, as they most surely will, necessity will offer an avenue for responding to cyber terrorism that does not reach the "armed attack" threshold necessary to act forcefully in self-defense.[48]

Because of the limitations on countermeasures and the necessity plea's high threshold, states may find their hands tied when needing to react to non-state hostile cyber operations. Unless the due diligence principle is extended to cyberspace, target states may find themselves permitted to respond only through law enforcement or by using diplomacy or retorsion to encourage the state from which hostile cyber operations are being launched (or where the cyber infrastructure being used is located, as in cases of remote control) to take action to end them. Hacking back would likely violate the sovereignty of the state into which the hack-back is conducted—an unsettled issue in international law that is also being examined in the Tallinn 2.0 process. And since that response would be attributable to the target state as a matter of law,

48. U.N. Charter art. 51; *see also* TALLINN MANUAL, *supra* note 8, at 54-61 (Rule 13).

ironically it could permit the state from which the initial cyber operations originated to conduct responsive countermeasures.

IV. THE BENEFITS OF THE DUE DILIGENCE PRINCIPLE IN THE CYBER CONTEXT

The principle of due diligence would provide states with a means to respond in the cases described above. If the territorial state fails to terminate an ongoing non-state cyber operation mounted from its territory against another state, and doing so is practical and reasonable in the circumstances, then the territorial state commits an internationally wrongful act by failing to exercise its obligations under the principle. The injured state would therefore have the right to take countermeasures against it, so long as those measures are consistent with state-responsibility conditions such as notice and proportionality.[49]

Recall that there is no requirement that countermeasures be directed against the state itself, although it must ultimately be the legal "interests" of the state with which the countermeasures interfere. Therefore, the injured state could launch cyber operations targeting the non-state actors that, but for their qualification as countermeasures, would violate the sovereignty of the state from which they are operating. The wrongfulness of that breach of sovereignty would be precluded by qualification of the operations as a countermeasure in response to the territorial state's breach of its due diligence obligation. The principle of due diligence would also permit the victim state to take countermeasures, whether cyber in nature of not, directly against a recalcitrant territorial state to compel it to take those measures necessary to terminate the non-state actor's operations.

A simple example illustrates operation of the approach. Assume the governmental CERT in state *A* identifies harmful cyber operations being mounted from defined private cyber infrastructure in state *B*. A non-state group with which state *B* is sympathetic claims responsibility for them. State *A* notifies state *B* of the harmful operations and requests its assistance in terminating them (which can feasibly be done), but the requests are ignored. Since state *B* is in breach of its due diligence obligation, state *A* is entitled to take countermeasures. It does so by conducting cyber operations that damage and shut down the cyber infrastructure being used by the non-state group. Even though the response would otherwise have violated state *B*'s sovereignty, its wrongfulness under international law is precluded by qualification as a countermeasure.

---

49. Articles on State Responsibility, *supra* note 29, at arts. 43, 51.

It is noteworthy that the due diligence principle would likewise provide grounds for a response when a state is suspected of engaging in the hostile cyber activities, but insufficient evidence exists to satisfy the level of certainty necessary for legal attribution. In other words, even where there is no smoking gun that would legally justify treating the cyber operations as those of the state, the state could be treated as having failed its due diligence obligation, and the principle would permit countermeasures on that basis. Employing the hook of due diligence would therefore enable remedial responses far more robust and effective than would otherwise be lawful.

CONCLUSION

As states consider their positions on applying the due diligence principle to cyber operations, they must carefully consider the consequences of opposing it. Yes, due diligence can impose a heavy burden on states. But international law acknowledges that the right of sovereignty and the corresponding duty of due diligence must be in equilibrium. As a matter of law, therefore, the due diligence obligation does not require a state to take measures that are beyond its means or otherwise unreasonable. A state need not undertake onerous measures to prevent its cyber infrastructure from being used maliciously, such as monitoring all cyber activity. And only when a state learns of ongoing activities—such as when the victim state brings it to light—does the duty mature. Most importantly, the principle of sovereign equality means that other states bear the same obligation. Thus, they have a legal incentive to ensure that harmful cyber operations are not conducted from their territories. If they fail to comply with their due diligence responsibility, the injured state may respond either directly against them or indirectly by conducting operations against the non-state actors involved.

Should states forfeit the remedies that the due diligence obligation provides by denying its application in cyberspace? Consider the DOD Cyber Strategy's pronouncement that "[i]n a manner consistent with U.S. and international law, the Department of Defense seeks to deter attacks and defend the United States against any adversary that seeks to harm U.S. national interests during times of peace, crisis, or conflict."[50] No state would adopt a contrary position. Thus, if they hope to effectively defend against *any* adversary during *times of peace* in a manner consistent with international law, states would do well to consider not only the costs of the principle, but also its benefits.

---

50. *The DoD Cyber Strategy*, *supra* note 38, at 2.

Preferred Citation: Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68 (2015), http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.