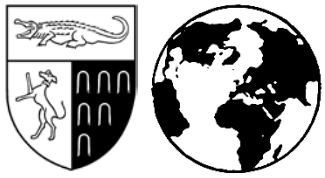
The Yale Journal of International Law Online



Grey Zones in the International Law of Cyberspace

Michael N. Schmitt†

INTRODUCTION

In 2015 and 2016, hackers affiliated with the Russian government broke into servers of the U.S. Democratic National Committee (DNC).[1] The subsequent release of documents hurt Democrats in Congressional races, led to the resignation of the DNC Chairperson, created tension between the Clinton and Sanders camps, and, above all, figured prominently in the race for president.[2] The Russian operations were yet another example of Russia's proficiency at exploiting the "grey zones" of international law, which it had honed during operations that led to the belligerent occupation of the Crimean Peninsula and its support for insurgent forces in eastern Ukraine.

By this strategy, Russia exploits international law principles and rules that are poorly demarcated or are subject to competing interpretations. With respect to its activities in Ukraine, Russia played on the legal margins by masking its direct involvement in the hostilities, which would have implicated the *jus ad bellum* use of force prohibition[3] and openly initiated an international armed conflict between Russia and Ukraine under the *jus in bello*.[4] In doing so, Russia

† Professor of International Law, University of Exeter; Chairman, Stockton Center for the Study of International Law, U.S. Naval War College; Francis Lieber Distinguished Scholar, U.S. Military Academy at West Point. The author directed the Tallinn Manual Project from 2009-2017. The views expressed are those of the author in his personal capacity.

1. Dir. Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, U.S. SENATE SELECT COMM. ON INTELLIGENCE 2 (Jan. 6, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

2. Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

3. U.N. Charter art. 2(4). On the customary international law character of the prohibition, see Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S) (*Nicaragua*), Judgment, 1986 I.C.J. 14, ¶¶ 188-90 (June 27).

4. Common Article 2 of the 1949 Geneva Conventions sets forth the accepted standard for an international armed conflict. Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, Aug. 22, 1864, 22 Stat. 940, 1 Bevans 7; Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75

refocused attention on the complex questions of State responsibility for the actions of non-State actors[5] and the level of control under international humanitarian law that internationalizes a non-international armed conflict.[6]

The DNC hacks epitomized the grey zone strategy. The legal issue posed was whether the operations amounted to either a breach of U.S. sovereignty or a prohibited intervention under international law, topics addressed below.[7] As to the former, some current and former highly-placed U.S. government officials have recently questioned whether sovereignty is a primary rule of international law—that is, a rule that can itself be breached.[8] With respect to the latter, the operations had to be intended to "coerce" the United States before qualifying as prohibited intervention.[9] It is unclear whether facilitating the release of actual e-mails—as distinct from, for example, using cyber means to alter election returns—amounts to coercion as a matter of law. Such normative uncertainty provided fertile ground upon which the Russians could conduct their operations.

By acting within legal grey zones, Russia makes it difficult for other States to definitively name and shame the country as having committed an internationally wrongful act.[10] Legal ambiguity also hobbles responses. Had the DNC hacks plainly been unlawful under international law, the United States would have been entitled to take "countermeasures," actions that are unlawful but for the fact that they respond to another State's unlawful action. In this case, the Obama administration could have employed countermeasures, like hack backs, to disrupt Russian government and private cyber activities. Instead, the U.S. government resorted to the expulsion of 35 diplomats and the imposition of limited sanctions.[11]

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 art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention (III) Relative to the Treatment of Prisoners of War art. 2, 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 art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

5. *See* G.A. Res. 56/83, annex, art. 8, Responsibility of States for Internationally Wrongful Acts (Jan. 28, 2002) [hereinafter Articles on State Responsibility] ("The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.").

6. This requisite level of control is generally understood to be "overall control" of an organized armed group. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶¶ 131-140, 145, 162 (Intl'l Crim. Trib. for the Former Yugoslavia July 15, 1999) [hereinafter Tadić Appeals Chamber Judgment]. On internationalization of conflict, see Dapo Akande, *Classification of Armed Conflicts: Relevant Legal Concepts*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS 32, 56-63 (Elizabeth Wilmshurst ed., 2012).

7. Espionage *per se* is not a violation of international law. However, the method by which it is accomplished may be unlawful, as when it violates the target State's sovereignty. *See* INT'L GROUP OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168 -74 (Rule 32) (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

8. Gary P. Corn, Jennifer M. O'Connor & Robert Taylor, *Sovereignty in the Age of Cyber*, AJIL UNBOUND (forthcoming). For the contrary position, see Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. (forthcoming 2017).

9. *Nicaragua*, 1986 I.C.J. at 107-08, ¶ 205.

10. The elements of an internationally wrongful act are attribution and breach of an international legal obligation. Articles on State Responsibility, *supra* note 5, annex, art. 2.

11. As to the possibility that covert countermeasures might have been employed, note that there is a requirement of prior notice, since the purpose of countermeasures is to compel the State engaging in the unlawful conduct to desist. In situations where such notice is not feasible because of the necessity of an immediate response, or notice would allow that State to effectively defend against the countermeasures, post factum notice would still be required to convey the message that the State's unlawful conduct comes

In a sense, Russia's grey zone operations amount to a form of "asymmetrical lawfare." Its strategy is asymmetrical in the sense that States committed to the rule of law are less likely to operate in the grey zone than States that do not share this rule of law commitment. Thus, Russia has all the more reason to engage in legally ambiguous operations; it knows that its opponents may hesitate to react decisively, out of concern that their own response might be characterized as unlawful, opening the door to Russian claims of being the victim.[12] Compounding the situation is the fact that a target State's failure to respond at a commensurate level of severity—as in the weak U.S. response to Russian hacking—makes the attacker appear more powerful. In this asymmetrical dynamic, the State exploiting the grey zone accordingly tends to enjoy the advantage.

Fueling asymmetry is the fact that liberal democracies represent especially lucrative grey zone targets. As former President Tomas Ilves of Estonia perceptively noted, "Liberal democracies with a free press and free and fair elections are at an asymmetric disadvantage because they can be interfered with—the tools of their democratic and free speech can be used against them."[13] Such interferences often take place in the grey zones of international law.

This Essay identifies certain critical grey zones of international law that are susceptible to exploitation when conducting cyber operations. In doing so, it draws on the work of the two international groups of experts who prepared the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, published in 2013 and 2017, respectively.[14] The latter, which incorporates a slightly revised version of the former,[15] is the culmination of a seven-year project sponsored by the NATO Cooperative Cyber Defence Centre of Excellence that examined how international law applies in cyberspace. *Tallinn Manual 2.0* identifies scores of issues on which the expert opinions of the team diverged or there was lack of universal consensus. These disagreements demarcate much of the grey zones' landscape. Section II of the Essay highlights key grey zones that are particularly ripe for exploitation and in need of clarification by States. The catalogue is by no means exhaustive. States wishing to operate in the grey zones will seize opportunity wherever it presents itself. Finally, Section III concludes the Essay by proffering an approach that

---

at a cost. Therefore, covert countermeasures are more in the nature of retaliation, which is not a lawful purpose of countermeasures. *See* TALLINN MANUAL 2.0, *supra* note 8, at 116 (Rule 21); *see also id.* at 120 cmts. 10-12 (discussing the requirement of notification for countermeasures).

12. As noted by a U.S. intelligence officer, "It's not that the Russians are doing something others can't do . . . It's that Russian hackers are willing to go there, to experiment and carry out attacks that other countries would back away from." Sheera Frenkel, *The New Handbook for Cyberwar is Being Written by Russia*, BUZZFEED (Mar. 19, 2017), https://www.buzzfeed.com/sheerafrenkel/the-new-handbook-for-cyberwar-is-being-written-by-russia?utm_term=.jgOpW30jD#.kb0G6B2dL.

13. *Id.*

14. INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0]; TALLINN MANUAL 2.0, *supra* note 7.

15. In this Essay, references to the "views of the experts" refer to the group of experts that handled the matter. The first group (*Tallinn Manual 1.0*) addressed the use of force and humanitarian law issues raised in this Essay, whereas the second (*Tallinn Manual 2.0*) dealt with the other matters. Because *Tallinn Manual 2.0* incorporates the slightly revised text of the first manual, references herein are to the latter publication.

would narrow the grey zones so as to enhance normative stability in cyberspace. It also offers final thoughts on the benefits of such narrowing.

I. KEY GREY ZONES

A. Sovereignty

Of all international law principles, sovereignty is perhaps the most fundamental. From that principle emerges, *inter alia*, notions of non-intervention; prescriptive, enforcement, and adjudicative jurisdiction; sovereign immunity; due diligence; and territorial integrity. Max Huber set forth the classic definition of sovereignty in his 1928 *Island of Palmas* arbitral award: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[16]

Sovereignty has both an internal and external component. Internal sovereignty refers to the right of a State to exercise its control over persons, including legal persons, objects, and activities on its territory. It is incontrovertible that this right extends to control over individuals engaged in cyber activities, cyber infrastructure located on a State's territory, and any cyber activities that occur in or through that territory.[17] For instance, a State is entitled to exercise prescriptive jurisdiction to promulgate legislation and regulations governing cyber operations emanating from its territory.[18] This authority extends to both public and private persons and cyber infrastructure[19] and applies irrespective of the nationality of the natural or legal persons involved.[20] It is, however, subject to specific carve outs in international law, such as the protections of international human rights law.[21]

External sovereignty, by contrast, refers to the right of States to engage in international relations, as in the case of conducting diplomacy and entering into international agreements.[22] For example, in the exercise of external sovereignty a State is free to, or not to, become Party to a treaty governing cyber activities. Such sovereignty is also the basis for the legal immunity of States.[23] As with internal sovereignty, the existence of external sovereignty is not in dispute.

There are, however, two significant grey zones with respect to sovereignty. The first is a novel contention that has only recently emerged. Its proponents argue that sovereignty is but a foundational principle that yields no sovereignty-specific primary rule of international law. Interestingly, that approach failed to

16. Island of Palmas (Neth. v. U.S.) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

17. *See* TALLINN MANUAL 2.0, *supra* note 7, at 13-16 (Rule 2) cmts. 1-12. The term "cyber infrastructure" as used in this Essay refers to "[t]he communications, storage, and computing devices upon which information systems are built and operate." *Id.* at 564.

18. *Id*. at 55 (Rule 9) cmt. 1.

19. *Id.* at 13-14 (Rule 2) cmt. 3.

20. *Id.* at 14 (Rule 2) cmt. 7.

21. *See id.* at 179-208 (Rules 34-38).

22. *Id*. at 16-17 (Rule 3).

23. *Id*. at 71-74 (Rule 12).

surface during the seven years of deliberations among the *Tallinn Manuals* experts. Nor did it play any role in the unofficial consultations with over 50 States and international organizations prior to publication of *Tallinn Manual 2.0*. However, writing in their personal capacity, three senior U.S. Department of Defense officials, two of whom have since left government, have argued that there is no prohibition on the violation of another State's sovereignty as such.[24] Instead, the activities of a State conducting cyber operations are only susceptible to violating other primary rules of international law, like non-intervention or the prohibition on the use of force. This position may mirror the one taken in a Department of Defense (DoD) legal memorandum that was released but then, after drawing attention, quickly designated "internal distribution only" by the then-General Counsel of the Department, Jennifer O'Connor, on the day before the inauguration of President Trump. This presumption that the positions overlapped is based on the fact that O'Connor is one of the three authors of the aforementioned piece. Additionally, the other two were the current Staff Judge Advocate of U.S. Cyber Command and the former DoD Principal Deputy General Counsel.

This "sovereignty as principle, but not rule" approach contradicts extensive State practice and *opinio juris* in the non-cyber context, which treat the prohibition as a primary rule, such that a violation of sovereignty would constitute an internationally wrongful act.[25] Moreover, there is no evidence that it represents the official position of the United States. Indeed, it would be surprising if it achieved that status since such a position would dismantle a key normative firewall safeguarding U.S. cyber infrastructure and activities. Nevertheless, considering the seniority of its proponents, the view has the potential to create a, hopefully temporary, grey zone within which other States could operate. For instance, the uncertainty created by this embryonic approach weakens arguments that North Korea's Sony hacks[26] or Russia's targeting of the DNC violated U.S. sovereignty.

The better, and prevailing, view is that sovereignty is the basis for a primary rule of international law by which the cyber operations of one State can violate the sovereignty of another. As noted by the International Court of Justice in its first case, *Corfu Channel*, "Between independent States, respect for territorial sovereignty is an essential foundation of international relations."[27] Central to this principle is the inviolability of territory, which protects against non-consensual actions on one State's territory by, or attributable to, another. The paradigmatic illustration in the cyber context is a close access operation involving the uploading of malware to cyber infrastructure using a USB flash drive.[28] There is also general agreement that a State may not conduct "inherently

24. Corn, O'Connor & Taylor, *supra* note 8.

25. *See* Schmitt & Vihul, *supra* note 8.

26. Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/.

27. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 35 (Apr. 9).

28. A possible exception is non-destructive cyber espionage while on another State's territory. A majority of the *Tallinn Manual 2.0* experts were of the view that conducting cyber espionage while physically present on another State's territory violates that State's sovereignty. However, some of the experts opined that the widespread practice of conducting espionage while abroad, although a violation of the target State's domestic law, creates a "carve out" in the law of sovereignty and therefore does not, in

governmental functions exclusively reserved to another State on the latter's territory,"[29] such as engaging in law enforcement without consent.[30] This prohibition would bar, for instance, a law enforcement officer of one State from conducting a search of databases through cyber means while in another State's territory.[31]

Despite this consensus, a substantial grey zone exists with respect to remote cyber operations conducted from outside the target State. The controversy does not involve remote operations that interfere with, or usurp, inherently governmental functions, because the target State undeniably enjoys an exclusive right to perform them on its territory.[32] A remote cyber operation causing physical damage or injury on another State's territory violates the latter's sovereignty, since the well-accepted notion of territorial integrity and inviolability is at its zenith when physical consequences manifest.[33] For instance, a cyber operation conducted by, or attributable to, a State that causes private infrastructure based in another State's territory to overheat, thereby damaging it, is a clear violation of sovereignty.

Below this threshold, a grey zone looms due to the lack of State practice and *opinio juris*. Some of the *Tallinn Manual 2.0* experts were of the view that the threshold for a violation of sovereignty should be drawn at physical damage or injury. However, a majority of them concluded that remotely causing cyber infrastructure's non-temporary loss of functionality is likewise a sovereignty violation, even if no physical damage occurs.[34] They correctly understood that there is little practical difference between physically damaging property and rendering it virtually inoperable.

Others took an even broader view but were unable to achieve any meaningful consensus as to precise criteria for a violation. Among the many possibilities tendered were "a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences . . . .; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation."[35] Resolution of this quandary through State practice and *opinio juris* is likely to take time; until then, hostile non-injurious or non-destructive cyber operations conducted into other

---

and of itself, amount to a sovereignty violation. TALLINN MANUAL 2.0, *supra* note 7, at 19 (Rule 4) cmts. 7-8.

29. *Id.* at 22-23 (Rule 4) cmt. 18.

30. *See, e.g.*, S.C. Res. 138, Question Relating to the Case of Adolf Eichmann (June 23, 1960). The resolution, adopted in the aftermath of the 1960 abduction of Nazi war criminal Adolph Eichmann from Argentina, declared that such acts affect sovereignty. *Id.* ¶ 1.

31. TALLINN MANUAL 2.0, *supra* note 7, at 22-23 (Rule 4) cmts. 16-18. A small grey zone exists with respect to the somewhat ambiguous term "inherently governmental functions," but certain situations are clear. Among those cited by the *Tallinn Manual* experts were "changing or deleting data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national events activities." *Id.* at 22 (Rule 4) cmt. 16.

32. *Id.* at 21-22 (Rule 4) cmt. 15.

33. *Id.* at 20 (Rule 4) cmt. 11. A few of the *Tallinn Manual 2.0* experts opined that physical damage or injury is but one factor in assessing whether a violation of sovereignty has occurred. *Id.* cmt. 12.

34. *Id.* at 20-21 (Rule 4) cmt. 13.

35. *Id.* at 21 (Rule 4) cmt. 14.

States' territory will benefit from the uncertainties surrounding the legal concept of a sovereignty violation.

B. Intervention

Intervention into the internal or external affairs of other States is an internationally wrongful act.[36] The rule of non-intervention is a natural derivative of the concept of sovereignty; to the extent that a State enjoys exclusive sovereign rights, other States necessarily shoulder a duty to respect them.[37] The International Court of Justice confirmed the prohibition in its *Nicaragua* judgment, where it observed, "The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law."[38]

There are two conditions precedent to finding a violation of the prohibition. Both are replete with vagueness that results in a wide grey zone. First, the prohibition only applies to matters that fall within another State's *domaine réservé*. As noted in *Nicaragua*, "[a] prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely."[39] These are matters that international law leaves to the sole discretion of the State concerned, such as the "choice of a political, economic, social and cultural system, and the formulation of foreign policy."[40] To illustrate, elections fall within the *domaine réservé*, such that using cyber means to frustrate them would raise issues of intervention. By contrast, purely commercial activities typically do not. Therefore, a State's cyber operations that are intended to afford business advantages to its national companies would not amount to intervention. Between these extremes, the scope of *domaine réservé* is indistinct. For instance, States generally enjoy an exclusive right to regulate online communication in the exercise of its sovereignty. Yet, the point at which international human rights law, such as the rights to freedom of expression or privacy,[41] takes domestic regulation beyond the confines of the *domaine réservé* remains unsettled.

---

36. *Nicaragua*, 1986 I.C.J. at 108, ¶ 205; TALLINN MANUAL 2.0, *supra* note 7, at 312 (Rule 66).

37. The prohibition of intervention "is the corollary of every state's right to sovereignty, territorial integrity and political independence." OPPENHEIM'S INTERNATIONAL LAW 428 (Robert Jennings & Arthur Watts eds., 1996).

38. *Nicaragua*, 1986 I.C.J. at 106-07, ¶ 202.

39. *Id*. ¶ 205. They are matters "not, in principle, regulated by international law." Nationality Decrees Issued in Tunis and Morocco, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 24 (Feb. 7).

40. *Nicaragua*, 1986 I.C.J. at 108, ¶ 205. *See also* G.A. Res. 2625 (XXV), annex, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (Oct. 24, 1970) [hereinafter Declaration on Friendly Relations] (discussing "[t]he principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter"); G.A. Res. 36/103, annex, ¶ 2(b), Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (Dec. 9, 1981).

41. *See, e.g*., G.A. Res. 217 (III) A, arts. 12, 19, Universal Declaration of Human Rights (Dec. 10, 1948); International Covenant on Civil and Political Rights arts. 17, 19(2), Dec. 16, 1966, S. EXEC. DOC. E, 95-2 (1978), 999 U.N.T.S. 171.

Second, to qualify as prohibited intervention, the act in question must involve coercion.[42] In the simplest terms, a coercive act is one designed to compel another State to take action it would otherwise not take, or to refrain from taking action it would otherwise engage in.[43] Coercion is accordingly more than mere influence. It involves undertaking measures that deprive the target State of choice.

Like *domaine réservé*, the precise parameters of coercion are less than definitive. Obviously, threatening or employing military force qualifies as coercion. In *Nicaragua*, the International Court of Justice found that "[t]he element of coercion . . . is particularly obvious in the case of an intervention which uses force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State."[44] In that case, the funding of insurgent forces was found to constitute prohibited intervention.[45] Analogously, funding a hacker group that engages in destructive cyber operations could qualify as intervention. At the other extreme, diplomacy and propaganda, albeit intended to cause another State to act in a certain manner, do not qualify as intervention because the target State retains the ability to choose; the decisions they are meant to affect remain voluntary, even though they may now be suboptimal.

The Russian hacks of the DNC servers offer a contemporary example of the grey zone surrounding coercion. Opinions vary as to whether the cyber operations were coercive in the intervention sense. The emails that were released had not been altered, and it is generally accepted that mere espionage, without more, is not unlawful under international law.[46] The opposing, and slightly sounder, view is that the cyber operations manipulated the process of elections and therefore caused them to unfold in a way that they otherwise would not have. In this sense, they were coercive. This grey zone surrounding coercion may have been the reason that the United States neither labelled the operations as unlawful nor took "countermeasures."[47] Of course, it is unknown what drove the U.S. response; perhaps it was a belief that the Russian actions were lawful, an uncertainty as to the state of the law, or even a U.S. desire to retain grey zone operations in its own kit bag.

C. Attribution

Under international law, States bear responsibility for the internationally wrongful cyber activities of their organs, such as the armed forces, intelligence services, and law enforcement agencies.[48] They are also legally responsible for

42. *Nicaragua*, 1986 I.C.J. at 108, ¶ 205.

43. TALLINN MANUAL 2.0, *supra* note 7, at 318-19 (Rule 66) cmt. 21.

44. *Nicaragua*, 1986 I.C.J. at 108, ¶ 205.

45. *Id*. ¶ 228.

46. *See* TALLINN MANUAL 2.0, *supra* note 7, at 168-74 (Rule 32).

47. The author's views on countermeasures are set forth in *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697 (2014).

48. *See* Articles on State Responsibility, *supra* note 5, annex, art. 4.

the acts of persons or entities that have been empowered by domestic law to "exercise elements of the governmental authority."[49] As an example, a State that contracts with a private company to engage in law enforcement activities by cyber means on another State's territory without that State's consent is itself responsible for any violation of the latter's sovereignty by the company. In both cases, the State is responsible, even if the acts in question are *ultra vires*.[50]

The grey zone with respect to attribution under the law of State responsibility tends to involve cyber operations that are conducted by non-State actors but are in some way linked to a State. For instance, consider the 2013 and 2014 Yahoo hacks that compromised over a billion accounts. The company asserted that the operations were "state-sponsored."[51] In terms of legal—as distinct from factual—attribution, the nonbinding yet authoritative International Law Commission's Articles on State Responsibility provide that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[52] Unfortunately, the notions of "instructions," "direction," and "control" all lack clarity.

The easiest concept to deal with is instructions. According to the commentary to the Articles on State Responsibility, instruction involves a non-State actor functioning as an auxiliary of the State.[53] Typically, the situation comprises the issuance of commands by the State to the non-State actor, such as a hacker group, to conduct a specific cyber operation. The activities concerned need not involve "elements of the governmental authority."

More problematic are the concepts of direction and control. The commentary suggests that the two should be viewed disjunctively,[54] but it does not elucidate the difference between them. Similarly, international tribunals have failed to distinguish instructions, directions, and control with any degree of granularity. Instead, the prevailing approach tends towards a binary distinction in which either a State tells a non-State actor to perform an act (instruction or direction) or the State exercises "effective control" over the non-State actor with respect to the act in question.

The effective control test was first articulated by the International Court of Justice in its *Nicaragua* judgment[55] but was developed more fully by the court in the *Bosnian Genocide* case.[56] Speaking to the issue of attribution, the court noted:

---

49. *Id*. annex, art. 5.

50. *Id*. annex, art. 7.

51. Sam Thielman, *Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History*, THE GUARDIAN (Dec. 15, 2016), https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

52. Articles on State Responsibility, *supra* note 5, annex, art. 8.

53. UNITED NATIONS, MATERIALS ON THE RESPONSIBILITY OF STATES FOR INTERNATIONALLY WRONGFUL ACTS, U.N. Doc. ST/LEG/SER.B/25 (2012), ¶ 2 of commentary to art. 8.

54. See *id.*, ¶ 7 of commentary to art. 8.

55. *Nicaragua*, 1986 I.C.J. at 64-65, ¶ 115.

56. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro) (*Bosnian Genocide*), Judgment, 2007 I.C.J. 43 (Feb. 26).

> [I]t is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of "complete dependence" on the respondent State; it has to be proved that they acted in accordance with that State's instructions or under its "effective control". It must however be shown that this "effective control" was exercised, or that the State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[57]

The court rejected the less stringent "overall control" test adopted by the International Criminal Tribunal for the former Yugoslavia in the *Tadić* case.[58] It opined that "the 'overall control' test has the major drawback of broadening the scope of State responsibility well beyond the fundamental principle governing the law of international responsibility: a State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf."[59]

Thus, if the degree of control does not reach the overall level, it does not necessarily rise to that of effective control. Since the Yugoslavia tribunal observed that overall control involved more than "the mere financing and equipping of such forces" and should include "planning and supervision of military operations,"[60] financing and providing malware to a non-State hacker or terrorist group that carries out hostile cyber operations against another State would not suffice for attribution. Nor would the threshold be crossed if the group conducts cyber operations merely to please the State, express support for it, or enhance or facilitate its cyber operations without being asked to do so, since none of these examples would involve "control."

The key is actual control over the cyber operations themselves. Herein lies the grey zone, for the law remains imprecise as to the nature and extent of the requisite control. It is reasonable to interpret the notion of effective control as denoting a State's *de facto* ability to cause the non-State actor to launch, terminate, or adjust the cyber operations in question. But would, for instance, a State's ability to withdraw financial or material support for a non-State group provide the requisite degree of control if withdrawal would considerably affect the group's ability to continue operating? In other words, although merely funding an operation may not suffice, is there a point at which the non-State group becomes so dependent on State support that the State essentially exercises effective control over whether and how the group conducts its cyber operations? Similarly, can providing sanctuary for a non-State group be interpreted as effective control over the group's cyber activities when that group would not survive without sanctuary? Absent either express instructions to engage in a cyber operation or integration into the State's formal or informal command structure, it will be difficult to conclusively attribute a non-State actor's cyber operations based on a State's control over it, except in the most obvious of cases.

---

57. *Id.* ¶ 400.
58. Tadić Appeals Chamber Judgment, *supra* note 6, ¶ 137.
59. *Bosnian Genocide*, 2007 I.C.J. at 210, ¶ 406.
60. Tadić Appeals Chamber Judgment, *supra* note 6, ¶ 145.

D. Due Diligence

Pursuant to the principle of due diligence, States are obligated to ensure that their territory is not used for purposes detrimental to the rights of other States. As noted by the International Court of Justice in the *Corfu Channel* case, it is "every State's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other States."[61]

The *Tallinn Manual 2.0* experts agreed that this principle applies to cyber operations emanating from a State's territory.[62] For example, during the 2007 widespread hostile cyber operations against Estonia, most of which originated from Russian territory, Russia breached this obligation by failing to take action to terminate them after it became aware of the electronic onslaught.[63] However, because not every State involved in pre-publication consultations readily accepted the application of due diligence to cyberspace as a matter of customary law, the *Tallinn Manual 2.0* acknowledges a view by which the premise of applicability is *lex ferenda* (what the law should be), rather than *lex lata* (current law).[64] This position is based in part on the 2013 and 2015 reports of the United Nations Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). In the reports, the GGE stated that States "should," rather than must, take those actions necessary to put an end to cyber operations harmful to other States emanating from the formers' territories.[65] As due diligence is purportedly a primary rule of international law, a State's violation of which constitutes an internationally wrongful act, such hesitancy to accord the rule *lex lata* status produces a grey zone of international law.

Contributing to that zone is the fact that the *Tallinn Manual 2.0* experts were sometimes divided as to the interpretation of the due diligence obligation. All agreed that it applies when cyber operations having serious adverse consequences vis-à-vis a legal right of a State are mounted from another State's territory. This standard, however, raises a number of issues that broaden the grey area.

First, the term "serious adverse consequences," which the experts borrowed from international environmental law,[66] is undefined in international law.

---

61. *Corfu Channel*, 1949 I.C.J. at 22. *See also* S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 88 (Sept. 7) (Moore, J., dissenting) ("It is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people."); *Island of Palmas*, 2 R.I.A.A. at 839 ("Territorial sovereignty . . . involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States . . . .").

62. TALLINN MANUAL 2.0, *supra* note 7, at 30 (Rule 6).

63. On the incident, see ENEKIN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14-34 (2010), https://ccdcoe.org/publications/books/legalconsiderations.pdf.

64. TALLINN MANUAL 2.0, *supra* note 7, at 31 (Rule 6) cmt. 3.

65. Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomm. in the Context of Int'l Sec., U.N. Doc. A/68/98, ¶ 23 (June 24, 2013) [hereinafter 2013 GGE Report]; Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomm. in the Context of Int'l Sec., U.N. Doc. A/70/174, ¶¶ 13(c), 28(e) (July 22, 2015) [hereinafter 2015 GGE Report].

66. *See* Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941) ("[N]o State has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of

Moreover, seriousness is typically understood as contextual in nature, and contextuality generally leads to ambiguity. A few experts even argued that the standard set the threshold too high and instead proposed use of the term "significant" in lieu of "serious."[67]

Botnets pose unique issues vis-à-vis the due diligence obligation.[68] Many cyber operations launched from one State against another are conducted by means of a botnet. The individual bots that make up the botnets may be located in many countries. This raises the question of whether the requirement of serious adverse consequences refers to the aggregate consequences caused by the botnet or only to those consequences caused by the bots in the State that may have the due diligence obligation. A minority of the *Tallinn Manual 2.0* experts, approaching the matter from the perspective of a State suffering the harm, adopted the former view,[69] whereas the majority, addressing it from that of a State shouldering the due diligence obligation, supported the latter. The majority did so on the basis that "the other approach would create an imbalance between the right to control territory and the duty to ensure it is not used to harm other States."[70] It is the more principled approach in law.

Second, the requirement that the consequences involve the legal right of another State fuels grey zone issues generally. As discussed, there is a degree of controversy surrounding the assertion of violation of sovereignty as a primary rule. If it is not a primary rule, operations that would otherwise breach it would not fall within the ambit of the due diligence obligation. Similarly, recall the uncertainty as to the element of coercion in prohibited intervention. Should the coercive element not be satisfied by an operation mounted from a State's territory, that State would have no due diligence obligation to put an end to the operation, absent violation of another primary rule of international law.

Third, during pre-publication consultations, several States expressed concern as to the burden they would have to shoulder if a cyberspace due diligence duty represents a binding, as distinct from hortatory, norm. This concern was misguided because the obligation is one of conduct, not of result. The sole requirement is that a State take those measures that are feasible in the attendant circumstances.[71] There are two key factors in this regard: the technical wherewithal of the territorial State to put an end to the offending operations, and the sheer number of offending operations with which some States must deal. Of course, because it is subjective and contextual, the feasibility standard contributes to the grey zone.

Fourth, there is a lack of certainty with respect to whether the due diligence obligation applies only to the States from which the offending cyber operations

---

another or the properties or persons therein, when the case is of *serious consequence* and the injury is established by clear and convincing evidence.") (emphasis added).

67. TALLINN MANUAL 2.0, *supra* note 7, at 36-37 (Rule 6) cmt. 25.

68. *Tallinn Manual 2.0* defines botnet as: "A network of compromised computers, so-called 'bots', remotely controlled by an intruder, 'the botherder', used to conduct coordinated cyber operations, such as 'distributed denial of service' operations. There is no practical limit on the number of bots that can be assimilated into a botnet." *Id.* at 563.

69. *Id.* at 38-39 (Rule 6) cmts. 29-31.

70. *Id.* cmt. 30.

71. *Id.* at 43 (Rule 7).

are mounted, or whether it also imposes obligations on those through which they transit. In the first edition of the *Tallinn Manual*, the experts did not achieve consensus on the issue, primarily because of the technical difficulty of identifying and terminating the operations.[72] The experts responsible for the *Tallinn Manual 2.0*, having received advice from technical experts that it is sometimes possible for transit States to identify and block harmful cyber operations, concluded that "as a strict matter of law, the 'transit State' shoulders the due diligence obligation and must act pursuant to Rule 7 when it (1) possesses knowledge (on actual and constructive knowledge . . . .) of an offending operation that reaches the requisite threshold of harm and (2) can take feasible measures to effectively terminate it."[73] The group's hesitancy in adopting a transit State obligation signals that the issue of such an obligation, and its application in particular circumstances is likely to remain controversial.

Finally, the experts agreed that the due diligence obligation attaches when cyber operations are being conducted or are imminent and have serious adverse consequences for another State. However, as applied in international environmental law, the principle is sometimes treated as having a preventative element.[74] The *Tallinn Manual 2.0* experts concluded that there is no preventive duty with respect to cyber operations that would require a State to, for instance, monitor ongoing cyber operations from its territory or take measures to ensure the cyber hygiene of cyber infrastructure that a State or non-State actor might take control of to mount the operations.[75] They did acknowledge a contrary view,[76] the existence of which raises grey zone considerations.

E. The Use of Force and Self-Defense

Article 2(4) of the United Nations Charter provides: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations." This fundamental rule of international law is universally recognized as customary in nature,[77] and widespread consensus exists that it applies fully to cyber operations conducted by or attributable to States.[78] There is, however, significant uncertainty as to where the use of force threshold lies.

---

72. TALLINN MANUAL 1.0, *supra* note 14, at 28-29 (Rule 5) cmt. 12.

73. TALLINN MANUAL 2.0, *supra* note 7, at 33 (Rule 6) cmt. 13.

74. Int'l Law Comm'n, Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, art. 3, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 372 (2001).

75. TALLINN MANUAL 2.0, *supra* note 7, at 41-42 (Rule 6) cmt. 42; *id.* at 44-45 (Rule 7) cmts. 7-10. The experts looked to the *Bosnian Genocide* case in drawing this conclusion: "A State's obligation to prevent, and the corresponding duty to act, arise at the instant that the State learns of . . . the existence of a serious risk that the act [of genocide] will be committed." *Bosnian Genocide*, 2007 I.C.J. at 183, ¶ 431.

76. TALLINN MANUAL 2.0, *supra* note 7, at 46 (Rule 7) cmts. 12-13; *see also Corfu Channel*, 1949 I.C.J. at 44 (opinion of Alvarez, J.).

77. *Nicaragua*, 1986 I.C.J. at 99-101, ¶¶ 188-90.

78. TALLINN MANUAL 2.0, *supra* note 7, at 329 (Rule 68).

It appears to be settled that a cyber operation causing physical damage or injury qualifies as an unlawful use of force except when otherwise authorized in international law, such as in the case of self-defense; authorization,[79] mandate or authorization by the United Nations Security Council pursuant to Chapter VII of the U.N. Charter;[80] or the affected State's consent.[81] The first edition *Tallinn Manual* experts concluded that certain operations not generating such consequences may also cross the use of force threshold.[82] They based their conclusion on the International Court of Justice's determination in the *Nicaragua* case, which held that arming and training guerrilla forces to fight against another State amounts to a use of force against that State.[83] Applying this finding by analogy, they agreed that providing malware and the training necessary to employ it against another State is a use of force.[84] When the relevant text of the first manual was reviewed for inclusion in *Tallinn Manual 2.0*, no subsequent State practice or *opinio juris* suggested a need for revision.[85]

Agreement on a bright line test for qualification of non-destructive or injurious cyber operations as a use of force proved elusive. This being so, the experts proposed an approach that assesses the likelihood of States characterizing a cyber operation as such. It is based "on the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition of the use of force."[86]

The method highlights factors that States are likely to focus on when making use of force determinations. Key ones include: severity of consequences; immediacy of consequences; directness of consequences; invasiveness of the operation; measurability of consequences; military character of the operation; extent of State involvement; and any presumptive legality on the type of operation, as in the case of psychological operations or espionage.[87] Other factors that the experts identified as relevant include: "the prevailing political environment, whether the cyber operation portends the future use of military force, the identity of the examiner, any record of cyber operations by the attacker, and the nature of the target."[88] With the exception of severity, no single factor alone is likely to qualify a cyber operation as a use of force. Instead, these and other factors are considered together when assessing the likelihood that the operation in question will qualify as a use of force.

79. U.N. Charter art. 51.

80. *Id.*, ch. VII.

81. *See* Articles on State Responsibility, *supra* note 5, annex, art. 20 ("Valid consent by a State to the commission of a given act by another State precludes the wrongfulness of that act in relation to the former State to the extent that the act remains within the limits of that consent.").

82. TALLINN MANUAL 1.0, *supra* note 14, at 45 (Rule 11) cmts. 4, 8.

83. *Nicaragua*, 1986 I.C.J. at 118-19, ¶ 228.

84. TALLINN MANUAL 2.0, *supra* 7, at 331-32 (Rule 69) cmt. 4.

85. *Id.* at 331-33 (Rule 69) cmts. 4, 8.

86. *Id.* at 333 (Rule 69) cmt. 8. This approach was initially proposed by the author in *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

87. TALLINN MANUAL 2.0, *supra* note 7, at 333-36 (Rule 69) cmt. 9.

88. *Id*. at 337 (Rule 69) cmt. 10.

The failure to achieve consensus on the use of force threshold, as well as the resulting decision of the experts to merely proffer an approach that considers a non-exclusive and contextual list of factors, indicates the extent to which the law surrounding the prohibition on the use of force constitutes a fertile grey zone for States. Somewhat less grey, albeit nevertheless unsettled, is the related matter of self-defense. Pursuant to Article 51 of the U.N. Charter, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." As with the prohibition on the use of force, there appears to be broad consensus that the article reflects customary international law[89] and applies to defense against cyber armed attacks.[90]

The key to understanding the right of self-defense in the cyber context is the meaning of the term "armed attack," which is undefined in international law. The prevailing view is that, while all armed attacks are necessarily uses of force, not all uses of force qualify as armed attacks. This was the International Court of Justice's approach in *Nicaragua*, where it distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[91] It must be cautioned that the United States continues to maintain that there is no difference between the use of force and armed attack thresholds. This contention, which is not widely accepted, contributes to the grey zone regarding self-defense.[92]

For other States, the challenge lies in identifying those cyber uses of force that are "most grave." Self-evidently, "a cyber operation that seriously injures or kills a number of persons or that causes significant damage to or destruction of property would satisfy the scale and effects requirement."[93] Below this threshold, consensus quickly fades. Indeed, the first edition *Tallinn Manual* experts were divided over whether the 2010 Stuxnet operation, which damaged Iranian centrifuges, qualified as an armed attack, although they agreed that the

89. *Nicaragua*, 1986 I.C.J. at 102-03, ¶ 193; Legality of the Threat or Use of Nuclear Weapons (*Nuclear Weapons*), Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8); Oil Platforms (Iran v. US), Judgment, 2003 I.C.J. 161, ¶¶ 51, 74, 76 (Nov. 6); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (*Wall*), Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9).

90. TALLINN MANUAL 2.0, *supra* note 7, at 339 (Rule 71). This conclusion is based on the International Court of Justice's determination that Article 51 applies to "any use of force, regardless of the weapon used." *Nuclear Weapons*, 1996 I.C.J. at 244, ¶ 39; *see also* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *in* 54 HARV. INT'L L.J. ONLINE 1, 4 (2012), http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf; Brian Egan, Legal Adviser, U.S. Dep't of State, International Law and Stability on Cyberspace, Remarks at Berkeley Law School (Nov. 10, 2016).

91. *Nicaragua*, 1986 I.C.J. at 101, ¶ 191.

92. *See, e.g.*, OFFICE OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., LAW OF WAR MANUAL 1017, ¶ 16.3.3.1 (Dec. 2016); *see also* Koh, *supra* note 90, at 4; William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE J. INT'L L. 295, 299-302 (2004); Abraham D. Sofaer, *International Law: Terrorism, the Law, and the National Defense*, 126 MIL. L. REV. 89, 93-96 (1989). All three authors served as Legal Adviser to the U.S. Department of State.

93. TALLINN MANUAL 2.0, *supra* note 7, at 341 (Rule 71) cmt. 8.

operation rose to the level of a use of force.[94] Some experts contended that a cyber operation must cause physical damage or injury in order to rise to the level of an armed attack. Others, correctly so, were less concerned with the nature of the consequences and focused instead on their severity.[95] For instance, States are arguably likely to consider a devastating attack on their economic system as an armed attack, because they will not countenance being limited to responses that lie below the use of force level permissible only in self-defense.[96]

Further complicating matters are situations involving a series of cyber operations, none of which alone crosses the armed attack threshold. There, the relevant question would be whether a State may aggregate the consequences of individual operations such that they cumulatively reach the armed attack threshold, a particularly relevant question if the severity approach just mentioned is adopted. In the view of the experts, aggregation is appropriate when a single State or group is the author of all the operations. The experts would also allow for aggregation when multiple States or groups act in concert.[97] However, because international law does not address this issue and there is little State practice or *opinio juris* to date, their conclusion is speculative.

An additional topic contributing to the self-defense grey zone is whether non-State actors may, as a matter of law, conduct an armed attack in situations where their cyber operations cannot be attributed to a State. In the aftermath of the 9/11 attacks, the international community appeared to treat Al Qaeda's operations as an armed attack, activating the right of self and collective defense.[98] Doing so was consistent with the text of Article 51, which makes no reference to States specifically as the initiators of the requisite armed attack. Because the issue surrounds the actor rather than the cyber character of the operations, some States,[99] academics,[100] and the majority of the *Tallinn Manual* experts[101] have agreed that the same logic applies to cyber operations mounted by non-State groups.

---

94. *Id*. at 342 (Rule 71) cmt. 10. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (discussing Stuxnet in greater detail).

95. TALLINN MANUAL 2.0, *supra* note 7, at 342-43 (Rule 71) cmt. 12.

96. *See* GOV'T OF THE NETH., GOVERNMENT RESPONSE TO AIV/CAVV REPORT ON CYBER WARFARE 5 (2012) (adopting the conclusion of the Advisory Council on International Affairs that "if there are no actual or potential fatalities, casualties or physical damage," a cyber operation targeting "essential functions of the state could conceivably be qualified as an 'armed attack' . . . if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state." ADVISORY COUNCIL ON INT'L AFFAIRS AND THE ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, CYBER WARFARE at 21 (Dec. 2011); *See also* Koh, *supra* note 90, at 4; GOV'T OF THE U.K., RESPONSE TO HOUSE OF COMMONS DEFENCE COMMITTEE'S SIXTH REPORT OF SESSION 2012-13, at 7-8, ¶ 10 (Mar. 22, 2013).

97. TALLINN MANUAL 2.0, *supra* note 7, at 342 (Rule 71) cmt. 11.

98. *See, e.g*., S.C. Res. 1368 (Sept. 12, 2001); S.C. Res. 1373 (Sept. 28, 2001); Press Release, N. Atl. Treaty Org., Statement by the North Atlantic Council (Sept.12, 2001); CONSULTATION OF MINISTERS OF FOREIGN AFFAIRS, ORG. OF AM. STATES, TERRORIST THREAT TO THE AMERICAS, OAS Doc. RC.24/RES.1/01 (2001).

99. *See, e.g.*, DEP'T OF DEF., LAW OF WAR MANUAL, *supra* note 92, at 1018 ¶ 16.3.3.4; GOV'T OF THE NETHERLANDS RESPONSE, *supra* note 96, at 5.

100. ADVISORY COUNCIL ON INT'L AFFAIRS & THE ADVISORY COMM. ON ISSUES OF PUB. INT'L LAW, CYBER WARFARE at 21-22 (Dec. 2011).

101. TALLINN MANUAL 2.0, *supra* note 7, at 345 (Rule 71) cmt. 18.

However, the International Court of Justice questioned this approach in its Armed Activities judgment and *Wall* advisory opinion.[102] In those cases, the court appeared unwilling to extend the right of self-defense to situations in which the operations of the non-State groups could not be attributed to a State. The court has been fairly criticized, including by members of the court itself, for its hesitancy to interpret the right as encompassing attacks by non-State actors, especially in light of the State practice and *opinio juris* to that effect.[103] Yet, its pronouncements lend an air of uncertainty to the assertion of a right of self-defense against non-State actors who conduct cyber operations at the armed attack level.

F. Attacks in International Humanitarian Law

In the field of international humanitarian law (IHL), two issues have loomed large. Both concern the protection to which civilians and civilian objects are entitled during an international or non-international armed conflict.

The first issue is the meaning of the term "attack." Many IHL prohibitions are articulated by reference to the term. Key among these are the prohibitions on attacking civilians or civilian objects; the ban on indiscriminate attacks;[104] the rule of proportionality in conducting attacks;[105] and the requirement to take precautions in attack.[106] Whether these and other prohibitions and limitations apply to cyber operations depends on their qualification as attacks.

Additional Protocol I to the 1949 Geneva Conventions defines attacks as "acts of violence against the adversary, whether in offence or in defence."[107] Based on this definition, any cyber operation causing damage to objects or injury to individuals qualifies as an attack to which the IHL prohibitions and limitations apply. The definition seemingly would exclude, however, many cyber operations, such as the purported Russian attacks against Ukrainian power grids.[108] But this would run counter to the object and purpose of international humanitarian law in the sense that it is under-inclusive. In particular, it would appear incongruent to suggest that a kinetic attack causing physical damage to cyber infrastructure qualifies as an attack, but a cyber operation that renders the same infrastructure inoperative does not. In both cases, the effect is essentially the same: the user of the cyber infrastructure is deprived of its benefits.

---

102. *Wall*, 2004 I.C.J. at 194, ¶ 139; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶¶ 146-47 (Dec. 19).

103. *See, e.g.*, *Wall*, 2004 I.C.J. at 215, ¶ 33 (opinion of Higgins, J.); *id.* at 229-30, ¶ 35 (opinion of Kooijmans, J.); *id.* at 242-43, ¶ 6 (declaration of Buergenthal, J.); *Armed Activities*, 2005 I.C.J. at 337, ¶ 11 (opinion of Simma, J.).

104. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 51(2), 51(4), 52(1), June 8, 1977, 1125 U.N.T.S. 3, 26-27 [hereinafter Additional Protocol I]; 1 INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3, 25, 37 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter CUSTOMARY INTERNATIONAL HUMANITARIAN LAW].

105. Additional Protocol I, *supra* note 104, arts. 51(5)(b), 57(2)(a)(iii), 57(2)(b), 1125 U.N.T.S. at 26, 29; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 104, at 46.

106. Additional Protocol I, *supra* note 104, art. 57, 1125 U.N.T.S. at 29; CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 104, arts. 51-67.

107. Additional Protocol I, *supra* note 104, art. 49(1), 1125 U.N.T.S. at 25.

108. Frenkel, *supra* note 12.

Accordingly, a majority of the first edition *Tallinn Manual* experts took the view that interfering with the functionality of an object would constitute the damage necessary to make the cyber operation an attack to which the rules on attacks would apply.[109] However, views differed among the experts as to the requisite interference with functionality. Some took the position that to qualify, the cyber operation would have to necessitate physical replacement of the cyber infrastructure's components.[110] Others viewed sufficient interference of functionality as occurring when there is a need to reinstall an operating system or other data essential to the functioning of the cyber infrastructure.[111] Regardless of the approach adopted vis-à-vis functionality, many questions remain. For instance, is there a temporal dimension to the loss of functionality, such that a temporary denial of service operation does not qualify unless it results in physical damage or injury?

In this regard, the International Committee of the Red Cross (ICRC) has suggested that "an operation designed to disable an object—for example a computer or a computer network—constitutes an attack under the rules on the conduct of hostilities, whether or not the object is disabled through kinetic or cyber means." [112] It has also noted that "in order to differentiate between operations that amount to attacks and those that do not, it has been suggested that the criterion of 'inconvenience' should be relied upon."[113] But the ICRC has also cautioned, "what is covered by 'inconvenience' is not defined and this terminology is not used in IHL."[114] Thus, a significant grey area endures with respect to cyber attacks. Because attacks are the defining activity of armed conflict, and there is extraordinary reliance in modern societies on cyber activities, this grey zone represents an especially problematic conundrum.

Uncertainty likewise surrounds cyber operations directed at data. It is well accepted that when the destruction or alteration of data results in injury or damage, the cyber operation in question is subject to the full gamut of attack rules. However, the question is whether the data per se benefits from the protection that civilian objects enjoy. This depends on whether data is an object as a matter of law.

The first edition *Tallinn Manual* experts struggled with the issue,[115] and it has been the subject of an active debate among IHL experts.[116] On the one hand, treating data as a civilian object would prove over-inclusive because

109. TALLINN MANUAL 2.0, *supra* note 7, at 417 (Rule 92) cmt. 10.

110. *Id*.

111. *Id*. at 417-18 (Rule 92) cmt. 11.

112. INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS, REPORT ON THE 32ND INTERNATIONAL CONFERENCE OF THE RED CROSS AND RED CRESCENT 41 (2015).

113. *Id.* at 42.

114. *Id.*

115. TALLINN MANUAL 2.0, *supra* note 7, at 437 (Rule 100) cmts. 6-7.

116. *See, e.g.*, Heather Harrison-Dinnisson, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISR. L. REV. 39 (2015); Kubo Macak, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 ISR. L. REV. 55 (2015); Michael N. Schmitt, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 ISR. L. REV. 81 (2015).

doing so would bar some cyber operations that are well accepted in State practice, particularly psychological operations directed at the enemy civilian population. On the other hand, failure to treat data as an object falls short in the sense that doing so would open the door to cyber operations that could dramatically affect the civilian population, as in the case of a cyber attack against a State's electronic archives or its pension system.

A majority of the experts were of the view, drawing on the Vienna Convention on the Law of Treaties,[117] that the "ordinary meaning" of the term "object" could not be interpreted as necessarily including data, nor was there sufficient subsequent State practice or *opinio juris* to support its extension to data in either treaty law or as an interpretation of the equivalent customary law prohibition.[118] Their uneasiness over this conclusion was signaled by the unusual inclusion of the caveat that this is the case "in the current state of the law."[119] As with the ambiguity surrounding the term "attack," doubt regarding the legal character of data under IHL cuts at the heart of cyber operations during armed conflict because many such operations are designed to destroy, damage, or alter data.

III. THE WAY AHEAD

States have not been idle in the face of uncertainty as to the application of international law to cyberspace. Early suggestions by some States that international law does not apply to this new domain of international relations have since been widely rejected. Indeed, States have been working together over the past few years to identify norms of cyber behavior. Most notable in this regard is the work of the GGE, which initially consisted of representatives from fifteen States, including China, Russia, and the United States. In 2013, it published a consensus report confirming, "International 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 technologies (ICT)] environment."[120] The group agreed that "State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory." Furthermore, the group affirmed that human rights law applies to cyber activities, and, addressing the issue of attribution, that "States must not use proxies to commit internationally wrongful acts."[121]

In 2015 the GGE, which had grown to include representatives of twenty States, reaffirmed the points it had made two years earlier and added specific references to the principles of sovereign equality, peaceful settlement of disputes, non-intervention, and due diligence, although with respect to due diligence, the reference was framed in hortatory, rather than obligatory, terms. It also cited the

117. Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969, 1155 U.N.T.S. 331, 340.

118. TALLINN MANUAL 2.0, *supra* note 7, at 437 (Rule 100) cmt. 6.

119. *Id*.

120. 2013 GGE Report, *supra* note 65, ¶ 19.

121. *Id*. ¶¶ 20-23.

core principles of international humanitarian law and emphasized the prohibition on the threat or use of force. [122]

While these efforts largely settled the issue of international law's applicability to cyberspace and confirmed the relevance of its core principles and rules, they did not achieve the granularity necessary to shrink grey zones. Nor is establishing such granularity likely to occur given the typically slow pace of progress in multinational fora dealing with international law. Accordingly, it will likely be left to States to address grey zones through State practice and expressions of *opinio juris*. However, because most State practice in cyberspace is classified, the bulk of the heavy lifting will likely have to be accomplished by *opinio juris*. This may occur in the abstract, with States making general statements on legal issues that occupy the grey zones. Additional expressions of *opinio juris* could come through a State's justification of their cyber activities based on international law or a State's condemnation of other States' actions based on legal grounds.

Such statements may clarify the grey zone issues in two ways. First, when sufficient State practice and *opinio juris* exist to constitute "a general practice accepted as law," a new norm of customary international law crystallizes.[123] Yet, because the threshold for crystallization is high, it is more likely that grey zones will be narrowed through State expressions of *opinio juris* that clarify uncertainties or disagreements over the extant law. In this regard, *opinio juris* serves an interpretive function, rather than a law-creating one. Such expressions can also contribute to the interpretation of ambiguous treaty provisions, such as the meaning of the terms "use of force" and "armed attack" in Articles 2(4) and 51, respectively, of the U.N. Charter.[124]

This begs the question of whether the grey zones should be clarified. The argument is sometimes heard that States value ambiguity, as it affords them greater freedom of action in cyberspace. For instance, uncertainty over the nature of cyber operations that violate sovereignty not only lessens the likelihood that one's own remote operations will be styled as unlawful, but also lessens the risk that a target State will take countermeasures pursuant to the law of State responsibility. Similarly, ambiguity as to where the use of force threshold lies reduces the risk that a State's non-destructive or injurious cyber operations will be characterized as a violation of the use of force prohibition.

---

122. *See* 2015 GGE Report, *supra* note 65, ¶ 28.

123. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993. The lead case on customary international law is North Sea Continental Shelf Cases (Germ. v. Denmark; Germ. v. Neth.), Judgment, 1969 I.C.J. 3 (Feb. 20); *see also* Continental Shelf (Libyan Arab Jamahiriya v. Malta), Judgment, 1985 I.C.J. 13, ¶ 27 (June 3); COMM. ON THE FORMATION OF CUSTOMARY (GEN.) INT'L LAW, INT'L LAW ASS'N, STATEMENT OF PRINCIPLES APPLICABLE TO THE FORMATION OF GENERAL CUSTOMARY INTERNATIONAL LAW (2000); Yoram Dinstein, *The Interaction Between Customary International Law and Treaties*, 322 RECUEIL DES COURS (2006).

124. "Any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation" may be considered when interpreting treaty provisions. Vienna Convention on the Law of Treaties, *supra* note 117, art. 31(3)(b).

While this may be so, the principle of sovereign equality[125] means that a State seeking to exploit ambiguity may later find itself the victim of that very ambiguity. Indeed, opportunity is equally a risk in international law. Moreover, uncertainty can lead to escalation. Consider the case of a State that conducts a cyber operation in the belief that the operation does not amount to an internationally wrongful act. The target State responds with a countermeasure based on its assessment that the first operation constituted an internationally wrongful act. Because the first State believed it had acted lawfully, it might now interpret the countermeasure as escalatory. The same dynamic could operate, for instance, with respect to the meaning of the term armed attack in the law of self-defense. Grey zones constitute fertile ground for an escalatory spiral.

Clarification of grey zone issues will also enhance deterrence in cyberspace.[126] International law provides for set categories of responses to specified types of actions. Unfriendly but lawful cyber activities may be responded to by acts of retorsion.[127] Internationally wrongful cyber operations, on the other hand, may permit "injured" States to take cyber or non-cyber countermeasures.[128] Cyber operations amounting to an armed attack may be responded to with cyber or kinetic uses of force. Certitude that a cyber operation can risk consequences at a set level can deter the taking of that operation, because the State concerned cannot act in the hope that the target State will hesitate to respond out of concern that its response might be viewed as unlawful.

Ultimately, legal clarity breeds international stability. The brighter the redlines of international law as applied to cyber activities, the less opportunity States will have to exploit grey zones in ways that create instability. Although the international community is working together commendably to identify applicable norms for cyberspace, it will likely fall to States to imbue the law with sufficient specificity to effectively deprive those who would abuse grey zones for malevolent and destabilizing ends. It remains to be seen whether States will display the willpower to take on this important task.

125. U.N. Charter art. 2(1); Declaration on Friendly Relations, *supra* note 40, annex (proclaiming "[t]he principle of sovereign equality" and establishing that all States "have equal rights and duties and are equal members of the international community").

126. On deterrence in cyberspace, see Joseph S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SECURITY 44 (Winter 2016/17); LIAM NEVILL & ZOE HAWKINS, INT'L CYBER POLICY CTR., AUSTRALIAN STRATEGIC POLICY INST., DETERRENCE IN CYBERSPACE (2016).

127. Articles on State Responsibility, *supra* note 5, annex, art. 49.

128. *Id.* annex, arts. 22, 49-54.