ARTICLE

Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum*

Michael N. Schmitt·

· Director, Tallinn Manual Project; 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; Fellow, Harvard Law School Program on International Law and Armed Conflict; Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence. The views expressed are those of the author in his personal capacity. Although this article is the direct result of the work of the two International Group of Experts that produced *Tallinn Manual 2.0*, any conclusions, except as otherwise noted, do not necessarily represent those of any other member of the groups.

Abstract

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations examines the application of extant international law principles and rules to cyber activities occurring during both peacetime and armed conflict. It was intended by the two International Groups of Experts that drafted it to be a useful tool for analysis of cyber operations. The manual comprises 154 Rules, together with commentary explaining the source and application of the Rules.

However, as a compendium of rules and commentary, the manual merely sets forth the law. In this article, the director of the Tallinn Manual Project offers a roadmap for thinking through cyber operations from the perspective of international law. Two flowcharts are provided, one addressing state responses to peacetime cyber operations, the other analyzing cyber attacks that take place during armed conflicts. The text explains each step in the analytical process. Together, they serve as a *vade mecum* designed to guide government legal advisers and others through the analytical process that applies in these two situations, which tend to be the focus of great state concern. Readers are cautioned that the article represents but a skeleton of the requisite analysis and therefore should be used in conjunction with the more robust and granular examination of the subjects set forth in Tallinn Manual 2.0.

Table of Contents

Introduction

In 2007, Estonia was the target of widespread cyber operations in response to its movement of a Soviet-era statue commemorating the "Great Patriotic War" from the center of its capital, Tallinn. The following year, cyber operations figured prominently in the international armed conflict between Georgia and Russia.[1] As those incidents unfolded, it became clear that the international law community was ill-prepared to handle events in this new domain of conflict. Indeed, some commentators and states queried whether international law even applied to operations conducted in cyberspace.

To address the analytical void, the then-newly established NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), based in Tallinn, launched a multiyear project to assess the cyber relevance of the international law governing situations involving the "use of force," as that term is understood under the UN Charter and customary international law, as well as the applicability of international humanitarian law to cyber operations during armed conflicts. The project resulted in the 2003 publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare.[2] That year, the CCD COE commissioned a follow-on project to consider the peacetime legal regimes bearing on cyber operations. It culminated in the 2017 release of Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, which contains both the new material and the slightly revised text of the first edition.[3]

Tallinn Manual 2.0 has garnered global attention as states struggle with complex cyber operations mounted against their governments and private cyber infrastructure[4] by both other states and non-state actors. At the heart of this struggle is unfortunate uncertainty as to the applicable law. While there is no longer any serious debate as to whether international law applies to transborder cyber operations, the international community has been unable to achieve consensus on the precise application of many international law principles and rules that govern them. In great part, this is because states are conflicted.[5] A

---

[1] For an excellent analysis of these incidents, see ENEKEN Tikk, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 14–33 (2010).

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

[3] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0]. The term cyber operations refers to the "employment of cyber capabilities to achieve objectives in or through cyberspace. . . . [T]he term is generally used in an operational context." *Id*.

[4] TALLINN MANUAL 2.0 defines cyber infrastructure as "[t]he communications, storage, and computing devices upon which information systems are built and operate." *Id.* at Glossary.

[5] Russia's hack of the Democratic National Committee's servers is paradigmatic. In that case, the Obama Administration condemned Russian meddling in U.S. elections as "unacceptable" and stated it "would not be tolerated," but did not characterize the activity as unlawful. Moreover, the U.S. responses were acts of "retorsion" (see *infra*), which are available even without the actions to which they respond qualifying as "internationally wrongful acts. Clearly, the Administration

permissive view of international law would afford them leeway to conduct their operations abroad, but leave them without normative firewalls that will enhance their cyber security. Conversely, a permissive approach to international law's application to cyberspace could serve to restrain the cyber operations of other states and non-state actors, but comes at the cost of tying one's own hands.

The two so-called "International Group of Experts" (one each for the 2013 and 2017 editions) that produced the manuals operated in an environment designed to minimize such policy influences and concerns. The only state input occurred during the Dutch Ministry of Foreign Affairs sponsored "Hague Process," which facilitated unofficial feedback from over fifty states and international organizations on Tallinn Manual 2.0 drafts. The experts were therefore well-situated to provide an objective, albeit contextually informed, view of the international law of cyber operations. Tallinn Manual 2.0 does not answer every question related to these operations, but in a surprisingly large number of instances the International Groups of Experts achieved unanimity as to the applicable law and its interpretation. When consensus proved elusive, the experts catalogued all reasonable views on the matter, leaving it to states and the broader international law community to resolve over time.

The drafters of Tallinn Manual 2.0 intended it to be a useful starting point for analysis of cyber operations. However, it is only a compendium of rules and accompanying commentary. The manual does not serve as a roadmap for thinking through cyber operations. This article seeks to begin filling that void with two flowcharts, one addressing state responses to peacetime cyber operations, the other cyber attacks that take place during armed conflicts.[6] They are accompanied by commentary that discusses the relevant law. Together, they serve as a *vade mecum* designed to walk legal advisers and others through the analytical process that applies in these two situations, which tend to be the focus of most state concern. Users are cautioned that the article represents but a skeleton of the requisite analysis and therefore should be used in conjunction with the more robust and granular examination of the subjects set forth in Tallinn Manual 2.0.

I. State Responses to Harmful Cyber Operations

Whenever harmful or malicious cyber operations are launched from abroad against public or private cyber infrastructure, discussion quickly turns to the appropriate response. Unfortunately, statements by government officials and

---

understood the principle of "sovereign equality," by which characterization of the Russian actions as, for instance, a breach of sovereignty would have applied equally to analogous cyber activities by U.S. military and intelligence operations. *See* THE WHITE HOUSE, FACT SHEET: ACTIONS IN RESPONSE TO RUSSIAN MALICIOUS CYBER ACTIVITY AND HARASSMENT (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and.

[6] The flowcharts were developed by the author, Ms. Liis Vihul, CEO of Cyber Law International and formerly Research Scientist at the NATO Cooperative Cyber Defence Centre of Excellence, and Professor Wolff Heintschel von Heinegg of Viadrina-Europa University.

pundits are often counter-normative, a fact that tends to skew thinking as to whether, and if so how, the victim state should respond. In fact, international law sets forth clear typology of response options, with each option—self-defense, the plea of necessity, countermeasures, and retorsion—having its own conditions precedent. The first three countenance responses that would otherwise be unlawful, but for the nature and consequences of the cyber operation to which they respond.

A. *Self-defense*

When considering the range of responses available to states facing harmful cyber operations, it is necessary to begin by determining when those operations rise to the level of an "armed attack" under the *jus ad bellum*, for an armed attack is the *conditio sine qua non* of the right to engage in self-defense. The term is drawn from article 51 of the United Nations Charter, which provides "[n]othing 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. . . ."[7] There is universal agreement that the right of self-defense is also of a customary international law character.[8]

The right undeniably extends to armed attacks conducted by cyber means, a conclusion supported by the finding of the International Court of Justice (ICJ) that article 51 applies to "any use of force, regardless of the weapons employed,"[9] and by statements of states and international organizations.[10] Thus, when a state is the target of harmful cyber operations that rise to the level of an armed attack, it may respond with kinetic or cyber operations that would otherwise constitute prohibited uses of force in violation of article 2(4) of the UN Charter and its customary international law counterpart.[11] The challenge lies in determining whether a particular cyber operation amounts to an armed attack.

---

[7] U.N. Charter art. 51.

[8] *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US), 1986 I.C.J. 14, ¶¶ 176, 194 (June 27) [hereinafter Nicaragua]; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8) [hereinafter Nuclear Weapons]; Oil Platforms (Iran v. US), 2003 I.C.J. 161, ¶¶ 51, 74, 76 (Nov. 6); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9) [hereinafter Wall].

[9] Nuclear Weapons, 1996 I.C.J. 226, ¶ 39. *See also* Tallinn Manual 2.0, *supra* note 3, r. 71, para. 4.

[10] *See, e.g.*, NATO, WALES SUMMIT DECLARATION, para. 72 (Sept. 5, 2014); GOVERNMENT OF THE NETHERLANDS, GOVERNMENT RESPONSE TO AIV/CAVV REPORT ON CYBER WARFARE, para. 4 (last visited Mar. 30, 2017) [hereinafter DUTCH GOVERNMENT RESPONSE], https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/04/26/cavv-advies-nr-22-bijlage-regeringsreactie-en/cavv-advies-22-bijlage-regeringsreactie-en.pdf; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10, 13 (2011); U.S. DEP'T OF DEFENSE, OFFICE OF THE GEN. COUNSEL, LAW OF WAR MANUAL, para. 16.3.3 (last updated Dec. 2016) [hereinafter DOD MANUAL].

[11] U.N. Charter art. 2(4); Nicaragua, *supra* note 8, at ¶¶ 187–90. On the definition of a use of force in the cyber context, *see* TALLINN MANUAL, *supra* note 3, r. 69.

1. Armed attack

Certain armed attack criteria are clear-cut. For example, armed attacks are transborder in nature.[12] The paradigmatic case is a cyber operation mounted by, or attributable to (see below), one state against another. A transborder element also exists when non-state actors conduct cyber operations against a state by launching cyber operations remotely from another state's territory. By contrast, the concept of armed attack does not extend to cyber operations that are entirely domestic in character, as with harmful cyber operations mounted by a hacker group operating from within a state against private or public assets that are also located in that state.

In addition to having a transborder element, qualification of a cyber operation as an armed attack requires the resulting harm, or the harm that is intended to result, to reach a certain threshold of severity. It is clear that every armed attack at least must amount to a "use of force." This is evident from the ICJ's characterization of armed attacks as "the most grave forms of the use of force."[13] Yet, the precise use of force threshold is unclear. Although the International Group of Experts agreed that cyber operations resulting in physical damage or injury are unambiguously uses of force,[14] no consensus could be reached as to when cyber operations not having those consequences qualify. It only agreed, based on the ICJ's analogous finding in *Nicaragua* assessing state connections with non-state guerilla forces, that merely funding a non-state group that engages in forceful cyber operations is not a use of force, whereas providing malware and training in its use for such operations does qualify.[15] To address operations lying beyond these limited situations, and because they could agree on no bright-line test, the experts proffered a catalogue of non-exclusive factors that states might consider when deciding whether to characterize a cyber operation as a use of force.[16]

Complicating matters is the fact that the prevailing view, one consistent with the International Court of Justice's approach, is that while all armed attacks are uses of force, only the gravest uses of force are armed attacks.[17] There is no

---

[12] TALLINN MANUAL 2.0, *supra* note 3, r. 71, at para. 3.
[13] Nicaragua, *supra* note 8, at ¶ 191.
[14] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 69.
[15] Nicaragua, *supra* note 8, at ¶ 228.
[16] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 69, para. 9. The factors were based on the approach proposed in Michael N. Schmitt, *Computer Network and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914 (1999).
[17] *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE, paras. 550–54 (5th ed. 2011). The United States, in what is a relatively isolated position, is of the view that the armed attack threshold is identical to that of the use of force. *See, e.g.*, DOD MANUAL, *supra* note 10, para. 16.3.3.1; *see also* Abraham D. Sofaer, *International Law and the Use of Force*, 82 AM. SOC'Y INT'L L. PROC. 420, 422 (1988); Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-

question that a cyber operation causing significant physical damage or injury qualifies as grave.[18] However, this conclusion leaves unanswered the question of when does a cyber operation not generating such consequences rise to the armed attack level?

The International Group of Experts concurred that the answer lies in the "scale and effects" of the operation, a standard drawn from the *Nicaragua* judgment.[19] Unfortunately, the standard is, albeit accurate as a matter of law, of little practical use. It therefore will be for states, through practice and expressions of *opinio juris*, to imbue the concept of armed attack with substance through the development of a customary international rule.[20] Presumably, states will treat cyber operations with very severe consequences, such as the targeting of the state's economic well-being or its critical infrastructure, as armed attacks to which they are entitled to respond in self-defense. This will likely be the case even when those operations are neither destructive nor injurious.[21] Yet, until that occurs with sufficient density, the question will remain an open one.

2. Self-defense criteria

Assuming a cyber operation crosses the armed attack threshold, a state is only entitled to respond in self-defense if the operation is either imminent or ongoing.[22] The principle that states need not await the actual launch of an armed attack, but may act in self-defense anticipatorily, is well-accepted in international

---

Agency Legal Conference (Sept. 18, 2002), *reprinted in* 54 HARV. INT'L L. J. ONLINE, 4 (2012) [hereinafter Koh, Cyberspace].

[18] TALLINN MANUAL 2.0, *supra* note 3, r. 71, para. 8.

[19] Nicaragua, *supra* note 8, at ¶ 195.

[20] "Crystallization" of customary international law requires two elements—state practice (*usus*) and the conviction that said practice is engaged in, or refrained from, out of a sense of legal obligation (*opinio juris*). *See* Continental Shelf (Libyan Arab Jamahiriya v. Malta), Judgment, 1985 I.C.J. 13, ¶ 27 (June 3). On the requirements of customary international law, see North Sea Continental Shelf Cases (Germ. v. Denmark; Germ. v. Neth.), Judgment, 1969 I.C.J. 3 (Feb. 20). *See also* Int'l Law Ass'n, Final Report of the Committee on the Formation of Customary (General) International Law, Statement of Principles Applicable to the Formation of General Customary International Law, Report of the Sixty-Ninth Conference, London (2000); *see generally* Yoram Dinstein, *The Interaction Between Customary International Law and Treaties*, 322 Recueil des Cours (2006).

[21] In *this* regard, see the DUTCH GOVERNMENT RESPONSE, *supra* note 10, at 5, which adopted 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 International Affairs (Cyber Warfare, No. 77, AIV / No 22, CAVV, at 21 (Dec. 2011). *See also* Koh, Cyberspace, *supra* note 17, at 4 ["In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues."], and U.K. Government Response to House of Commons Defence Committee's Sixth Report of Session 2012–13, para. 10 (Mar. 22, 2013).

[22] TALLINN MANUAL 2.0, *supra* note 3, r. 73.

law,[23] although the point at which a prospective armed attack becomes imminent is not entirely settled. Traditionally, the standard was understood in terms of temporal proximity to the armed attack.[24] That standard may have been palatable in the past with respect to conventional operations, for the preparations for an attack were often observable by the target state, but it makes little sense in the context of cyber operations, which may be executed in milliseconds, with little warning and devastating effect.

Considering this reality, the better approach is reflected in what has become known as "the last window of opportunity" standard.[25] It requires the confluence of three factors. First, the prospective attacker must have the capability to mount a cyber operation at the armed attack level. Second, the attacker must intend to do so. The third requirement lies at the standard's heart. It allows the prospective victim of a forthcoming attack to employ defensive force, whether it be kinetic or cyber in character, only at the point that a failure to do so would forfeit its opportunity to effectively defend itself—in other words, in the state's last window of opportunity.[26]

Consider a situation in which a state has highly reliable evidence that another state is going to mount devastating cyber operations against it at some indefinite point in the near future. The state has drawn the reasonable conclusion that it will be unable to effectively foil the operations once they have commenced. In these circumstances, and without prejudice to other requirements of international law, the state may treat the armed attack as imminent and act to preempt it. It must be cautioned that the absence of any of the three

---

[23] *See, e.g.*, DEREK W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 188–189 (1958). Although imprecise as a strict matter of law, the right to act anticipatorily in self-defense is traditionally said to be reflected in the celebrated nineteenth century *Caroline* incident. Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 INT'L L. DIG. 412 (John Bassett Moore ed., 1906). *See also* Judgment of the International Military Tribunal Sitting at Nuremberg, Germany (Sept. 30, 1946), *in* 22 The Trial of German Major War Criminals: Proceedings of the International Military Tribunal Sitting at Nuremberg, Germany 435 (1950).

[24] *See generally* Terry D. Gill, *The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 113 (Michael N. Schmitt & Jelena Pejic eds., 2007).

[25] *See* discussion at TALLINN MANUAL 2.0, *supra* note 3, r. 73, paras. 4–5. For a state's adoption of the standard, see U.S. DEP'T OF JUSTICE WHITE PAPER, LAWFULNESS OF A LETHAL OPERATION DIRECTED AGAINST A U.S. CITIZEN WHO IS A SENIOR OPERATIONAL LEADER OF AL–QA'IDA OR AN ASSOCIATED FORCE 7 (n.d), http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf. An early proposal of the standard by the author was first set forth in Michael N. Schmitt, *Preemptive Strategies in International Law,* 24 MICH. J. INT'L L. 513, 534–36 (2003) [hereinafter *Preemptive Strategies*].

[26] The approach was developed by the author in Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 157 (Michael N. Schmitt & Jelena Pejic, eds., 2007).

aforementioned preconditions will render defensive action at the use of force level merely "preventive," and therefore unlawful.[27]

Actions in self-defense against a cyber armed attack must not be solely retaliatory. By the requirement of immediacy, once an armed attack is over, the right to engage in self-defense is extinguished.[28] Although this would appear to be an oft-insurmountable hurdle to acting in self-defense because cyber attacks can last mere moments, the requirement must be interpreted with sensitivity to the context in which it applies. Therefore, if the target state reasonably concludes that its attacker intends to conduct further cyber operations at the armed attack level, it may treat the operations in their entirety as an ongoing campaign against which it may take defensive action at any point.

A state that has been the victim of a cyber armed attack that is no longer underway and is unlikely to be repeated as one event in a campaign is not left without remedies. In such cases, the armed attack is certain to have constituted an "internationally wrongful act"[29] (unlawful under international law) for which reparations are likely available. Reparations include restitution, compensation, and satisfaction.[30] It should be noted that countermeasures (see below) may be taken to ensure that a state responsible for commission of an internationally wrongful act complies with any obligation to provide reparation.[31]

If hostile cyber operations at the armed attack level are imminent or ongoing, the victim state must next ascertain by whom the operations will be, or are being, conducted. When the author of the attack is another state, the victim state may respond forcefully in self-defense so long as doing so is consistent with the criteria of necessity and proportionality. These requirements have been acknowledged by the International Court of Justice and are accepted as customary in nature.[32]

A forceful response to a malicious cyber operation is "necessary" when non-forceful measures will not suffice to address the armed attack. For instance, if passive cyber defenses are effectively foiling the attack, the victim state may not

---

[27] TALLINN MANUAL 2.0, *supra* note 3, r. 73, para. 10.
[28] *Id.*, r. 73 and r. 73, at paras. 12–13.
[29] TALLINN MANUAL 2.0, *supra* note 3, r. 14; Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, art. 2, GA Res. 56/83 annex, UN Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter Articles on State Responsibility]. The Articles on State Responsibility are not binding law of themselves, but rather represent, in great part, an authoritative restatement of customary international law by the International Law Commission.
[30] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 29; Articles on State Responsibility, *supra* note 29, arts. 34–37. A state responsible for an internationally wrongful act may also be obligated to provide assurances and guarantees of non-repetition. TALLINN MANUAL 2.0, *supra* note 3*,* r. 27; Articles on State Responsibility, *supra* note 29*,* art. 30(b);
[31] Articles on State Responsibility, *supra* note 29, art. 49(1).
[32] See discussion of these requirements at TALLINN MANUAL 2.0, *supra* note 3, r. 72. *See also* Nicaragua, *supra* note 8, at ¶¶ 176, 194; Nuclear Weapons, *supra* note 8, at ¶ 41; Oil Platforms, *supra* note 8, at ¶¶ 43, 73–74, 76; Nuremburg Tribunal judgment, *supra* note 23, at 435.

launch cyber or kinetic responses that would amount to a use of force. Whereas the criterion of necessity deals with whether a forceful response is required to put an end to the harmful cyber operations, the proportionality criterion governs the scale and scope of that response.[33] A response that is clearly excessive relative to that needed to effectively defend against the armed attack is unlawful. As an example, if an attack may be defeated by conducting counter cyber or kinetic attacks against the cyber infrastructure from which it is being launched, it would be unlawful to conduct widespread operations at the use of force level against cyber infrastructure throughout the attacker's state.

3. Non-state actors.

Situations in which a non-state actor conducts harmful cyber operations at the armed attack level of severity against one state from another state's territory are legally more challenging. If the group is acting on behalf of a state, or a state is "substantially involved" in the operations, the victim state may treat the operations as an armed attack by the former state and employ necessary and proportionate cyber or kinetic force against both it and the group.[34] However, the law is unsettled as to situations in which non-state groups act on their own accord. Most members of the International Group of Experts took the position that their operations may, as a matter of law, qualify as armed attacks against which victim states may respond forcefully pursuant to their right of self-defense.[35] This view is supported by state practice in the non-cyber context[36] and has expressly been adopted by a number of states, including the United States, with respect to cyber attacks.[37]

In the estimation of the remaining experts, the right of self-defense is limited to situations in which the harmful cyber operations are conducted by, or attributable to, a state.[38] Advocates of this view typically cite the International Court of Justice's *Wall* advisory opinion and its judgment in the *Congo v. Uganda* as support.[39] In those cases, the ICJ, in the face of dissent from a number of its judges, seemed to suggest that absent attribution of a non-state group's activities

---

[33] TALLINN MANUAL 2.0, *supra* note 3, r. 72.
[34] TALLINN MANUAL 2.0, *supra* note 3, r. 71, paras. 16–17; Nicaragua, *supra* note 8, at ¶ 195.
[35] TALLINN MANUAL 2.0, *supra* note 3, r. 71, at paras. 19–20.
[36] *See, e.g.*, SC Res. 1368, UN Doc. S/RES/1368 (Sept. 12, 2001); SC Res. 1373, UN Doc. S/RES/1373 (Sept. 28, 2001); Press Release, NATO, Statement by the North Atlantic Council (Sept. 12, 2001); Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs, Terrorist Threat to the Americas, OAS Doc. RC.24/RES.1/01 (Sept. 21, 2001).
[37] *See, e.g.*, DOD MANUAL, *supra* note 10, at para. 16.3.3.4; *see also, e.g.*, DUTCH GOVERNMENT RESPONSE, *supra* note 10, at 5.
[38] TALLINN MANUAL 2.0, *supra* note 3, r. 71, at para. 19.
[39] Wall, *supra* note 8, at ¶ 139; Armed Activities in the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶¶ 146–47 (Dec. 19) [hereinafter Armed Activities].

to a state, the law of self-defense is inapplicable.[40] By this approach, a state facing even destructive or injurious cyber operations by a non-state actor may not rely on self-defense to justify a forceful response. Instead, it would have to base its response on another ground, such as protection of life under international human rights law.[41]

Assuming *arguendo* that a non-state actor's cyber operations may qualify as a cyber attack, the question remains as to whether a victim state may strike back at the group when it is operating from another state's territory without violating the latter's sovereignty or otherwise committing an internationally wrongful act. Here, the majority took the position, one asserted most forcefully by the United States, that conducting cyber operations into the territorial state to terminate a non-state actor's armed attack is permissible when the territorial state consents to such operations or is either "unable" or "unwilling" to put an end to the offending cyber operations.[42] The minority countered that such situations do not merit piercing the thick veil of sovereignty.[43]

When a single individual conducts harmful cyber operations at the armed attack level on behalf of a state, the attack may be attributed to the state for the purposes of the law of self-defense.[44] However, the International Group of Experts split over situations involving non-attributable cyber operations. Some of the experts took the view that self-defense against the individual is permissible, whereas others argued that the only lawful response is to be found in the law governing law enforcement.[45]

To summarize, pursuant to the law of self-defense, a forceful response, whether by cyber or other means, is unavailable in situations in which the hostile cyber operations do not reach the armed attack threshold. This is so even though

---

[40] *See, e.g.*, Wall, *supra* note 8, at ¶ 33 (separate opinion of Judge Higgins); *id.* at 229–30, ¶ 35 (separate opinion of Judge Kooijmans); *id.* at 242–43, ¶ 6 (declaration of Judge Buergenthal); Armed Activities, *supra* note 39, at ¶ 11 (separate opinion of Judge Simma).

[41] *See, e.g.*, Basic Principles on the Use of Force and Firearms by Law Enforcement Officials Adopted by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, Havana, Cuba, (Aug. 27–Sept. 7, 1990), http://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx.

[42] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 71, at paras. 25-26. On the U.S. position vis-à-vis the unwilling/unable approach, see Letter from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, U.N. Doc. S/2014/695 (Sept. 23, 2014); President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013); Office of the Press Sec'y, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013); U.S. DEP'T OF JUSTICE WHITE PAPER, *supra* note 25, at 1–2. For academic treatment of the subject, see Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VA. J. INT'L L. 483 (2012). For earlier treatment of the issue by the author, see *Preemptive Strategies*, *supra* note 25, at 540–43 (2003).

[43] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 71, at para. 25. *See also* IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 299–301 (1963).

[44] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 71, at para. 17.

[45] *Id.*, r. 71, at para. 20.

those operations may violate other aspects of international law, such as the requirement to respect the sovereignty of other states,[46] the principle of non-intervention,[47] and the prohibition of the use of force.

B. *The Plea of Necessity*

In such cases, the plea of necessity may be available as the basis for responding. In the vernacular of the law of state responsibility, necessity (as the term in used in this context rather than that of self-defense) is a "circumstance precluding wrongfulness."[48] It allows a state finding itself in a qualifying situation to respond in a manner that would otherwise be unlawful, as with a hack back that would violate the sovereignty of the state into which it is conducted.[49] An example would be a situation in which a terrorist group is launching operations from states that are powerless to act, perhaps because they lack the technical wherewithal to do so. Even though a target state's response against the group would otherwise be unlawful because of the response's effects in the other states, it may act pursuant to the plea of necessity so long as certain criteria described below are met.

The plea of necessity applies only to situations in which a cyber operation creates a "grave and imminent peril" to an "essential interest" of the state concerned,[50] although the harmful cyber operation on which the plea is based need not be an internationally wrongful act. This customary law remedy[51] is an acknowledgement that states should not be left without a viable response option in acute circumstances.

"Grave" peril suggests harm that is especially detrimental,[52] while "imminent" confirms that the state need not wait until said harm manifests, but instead may act anticipatorily.[53] "Essential" refers to a particularly important interest of the state and, accordingly, would rule out resort to the plea of necessity in most situations involving malicious cyber operations. The International Group

---

[46] *Id.*, rr. 1–5.
[47] *Id.*, rr. 66–67.
[48] *See* Articles on State Responsibility, *supra* note 29, ch. V, art. 25.
[49] *See* TALLINN MANUAL 2.0, *supra* note 3, r. 26.
[50] *See* Articles on State Responsibility, *supra* note 29, art. 25(1)(a).
[51] The principle of necessity has been expressly or impliedly cited by international tribunals and arbitral bodies on numerous occasions. *See, e.g.*, Wall, *supra* note 8, ¶ 140; Rainbow Warrior (NZ v. Fr.), 20 RIAA 217, ¶ 78 (Arb. Trib. 1990); LG&E Energy Corp. v. Argentina, ICSID Case No. ARB/02/1, decision on liability, ¶¶ 201–66 (Oct. 3, 2006); CMS Gas Transmission Co. v. Argentina, award, ICSID Case No. ARB/01/8, ¶¶ 304–394 (May 12, 2005); Enron Co. v. Argentina, award, ICSID Case No. ARB/01/3, ¶¶ 288–345 (May 22, 2007); Sempra Energy Int'l v. Argentine Republic, award, ICSID Case No. ARB/02/16, ¶¶ 325–39 (Sept. 28, 2007).
[52] *See, e.g.*, discussion in Gabčíkovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, ¶ 51 (Sept. 25) [hereinafter Gabčíkovo-Nagymaros].
[53] *Id.* at ¶ 54.

of Experts described such an interest as "one that is of fundamental and great importance to the State concerned."[54]

Necessity determinations are always contextual.[55] To illustrate, an operation targeting cyber infrastructure that supports the provision of medical care would not qualify as creating "grave" peril when sufficiently redundant systems exist to ensure the continued treatment of the population. Yet, if the healthcare system lacks resiliency, the operation may pose a significant risk to the population's well-being, thereby rendering the situation grave.

Assessments of essentiality are similarly contextual. In particular, it is difficult to characterize specific categories of infrastructure as essential in the abstract. Again, consider healthcare cyber infrastructure. A cyber operation could target aspects of that infrastructure that do not directly and severely impact the care of the population, as with that used for routine medical appointment scheduling. On the other hand, cyber operations could be directed at blood banks during a natural disaster with ensuing significant loss of life. In the first case, the effect on the healthcare infrastructure has not reached the essentiality threshold; in the second instance, it arguably has.

A state's formal designation of cyber infrastructure as "critical infrastructure"[56] is insufficient to render it essential for the purposes of the plea of necessity; the function it performs when viewed in light of the attendant circumstances at the time it is targeted drives the determination. As an example, the Department of Homeland Security's designation of election cyber infrastructure as critical infrastructure did not, *per se*, satisfy the essentiality requirement. Essentiality is a factual determination. Although it can be fairly argued that the integrity of the national electoral process is an essential interest of the United States, that is not a determination left to the U.S. government as a matter of international law.[57]

Even in situations in which cyber operations pose a grave and imminent threat to an essential interest of the state, the plea of necessity is subject to strict limitations. International law seeks to balance the rights and obligations of states, for they enjoy sovereign equality. Therefore, before the state may resort to the plea of necessity to justify a response that would otherwise be unlawful, that response must be the only means available to adequately safeguard the interest in

---

[54] Tallinn Manual 2.0, *supra* note 3, r. 26, para. 2.
[55] *Id.*, r. 26, para. 2; Articles on State Responsibility, *supra* note 29, art. 25, para. 15.
[56] "Critical infrastructure" includes "[p]hysical or virtual systems and assets of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment." *See* Tallinn Manual 2.0, *supra* note 3, at Glossary.
[57] Press Release, Dep't of Homeland Security, Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

question.[58] The response, moreover, may not affect the essential interest of any other state in a grave and imminent way.[59] In other words, states are precluded from addressing necessity situations if doing so would place any other state in comparable peril.

Despite the limitations, a major practical benefit of the plea of necessity is that actions based on the plea may be taken when a non-state group has mounted harmful cyber operations. There need be no relationship between the group and another state or attribution to another state if such attribution cannot be reliably confirmed. Actions may even be taken when the author of the operation is altogether unknown.[60] This distinguishes responses based on the plea of necessity from countermeasures, which are only available when the cyber operations to which they respond are conducted by, or otherwise attributable to, another state.[61]

C. *Countermeasures*

Countermeasures are responses by a state to the unlawful cyber operations of, or attributable to, another state that would be unlawful themselves but for the latter's conduct.[62] Their sole permissible purpose is to cause the latter (the "responsible state") to desist in wrongful cyber activities against the former (the "injured state"); retaliation and retribution are not motives that preclude the wrongfulness of a response.[63] Moreover, unlike operations based on necessity, countermeasures may only be conducted in response to internationally wrongful acts, which are actions or omissions that are both attributable to a state as a matter of law and breach an obligation owed another state.[64] Thus, whereas the plea of necessity precludes the wrongfulness of responses vis-à-vis states that are not responsible for having violated an obligation owed the injured state, or when

---

[58] Tallinn Manual 2.0, *supra* note 3, r. 26; Articles on State Responsibility, *supra* note 29, art. 25(1)(a).

[59] Tallinn Manual 2.0, *supra* note 3, r. 26, para. 2; Articles on State Responsibility, *supra* note 29, art. 25(1)(b). The author's views on the subject are set forth in Michael N. Schmitt and Christopher Pitts, *Cyber Countermeasures and Effects on Third Parties: The International Legal Regime,* 14 BALTIC YB INT'L L. 1 (2014).

[60] Tallinn Manual 2.0, *supra* note 3, r. 26, para. 11.

[61] Tallinn Manual 2.0, *supra* note 3, r. 20, para. 7.

[62] Tallinn Manual 2.0, *supra* note 3, r. 20; Articles on State Responsibility, *supra* note 29, art. 22. *See also* Nicaragua, *supra* note 8, ¶ 249; Gabčíkovo-Nagymaros, *supra* note 52, ¶¶ 82–83; Responsibility of Germany for Damage Caused in the Portuguese Colonies in the South of Africa (Naulilaa Arbitration) (Port. v. Ger.), 2 RIAA 1011, 1025–1026 (1928) (unofficially translated) [hereinafter Naulilaa]; Responsabilité de l'Allemagne en raison des actes commis postérieurement au 31 juillet 1914 et avant que le Portugal ne participât à la guerre ('Cysne') (Port. v. Ger.), 2 RIAA 1035, 1052 (1930); Air Services Agreement of 27 March 1946 (U.S. v. Fra.), 18 RIAA 416, ¶¶ 80–96 (1979) [hereinafter Air Services]. For the author's views on countermeasures and attribution, see Michael N. Schmitt, "*Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*," 54 VA. J. INT'L L. 697–732 (2014).

[63] Tallinn Manual 2.0, *supra* note 3, r. 21; Articles on State Responsibility, *supra* note 29, art. 49(1).

[64] Articles on State Responsibility, *supra* note 29, art. 2.

responsibility cannot be established, countermeasures are limited to taking action against responsible states. The key is attribution.

1. Attribution

It is necessary to distinguish between factual and legal attribution. Factual attribution refers to the degree of certainty that another state, or an entity for which that state is responsible, has launched the cyber operation. In international law, determinations of states as factual matters typically must be "reasonable," but there is no requirement that states be correct.[65] A majority of the International Group of Experts agreed that this is not the case with respect to countermeasures. States that take cyber or other countermeasures do so at their own risk.[66] Should a state misattribute a cyber operation to another state and take countermeasures in response thereto, it will itself be responsible for having committed an internationally wrongful act.

Legal attribution occurs pursuant to the law of state responsibility.[67] States are obviously legally responsible in international law for the acts of their organs, such as the armed forces, security services, and intelligence agencies.[68] Similarly, states are responsible for the acts of persons or entities that have been empowered under domestic law to exercise elements of governmental authority,[69] as in the case of a private cyber security company that a state has contracted to engage in cyber law enforcement activities like gathering evidence for criminal prosecution. In both of these cases, the acts are attributable to the state concerned even if they are *ultra vires*, that is, they exceed the actor's authority or contravene its instructions.[70]

In certain circumstances, the acts of other states or international organizations also may be attributable to a state.[71] Most attention in the cyber

---

[65] *See* Tallinn Manual 2.0, *supra* note 3, r. 71, para. 23.

[66] *Id.*, r. 20, para. 16; Articles on State Responsibility, *supra* note 29, art. 49, para. 3. The logic behind the difference is that countermeasures open the door to responses that would otherwise be unlawful. Other states should not be required to bear the risk of mistake, even reasonable ones, given this fact. However, at the armed attack level, the consequences of failing to act are severe enough that international law countenances the risk of mistake by only requiring states to act reasonably in the circumstances.

[67] For the author's views on attribution, see Michael N. Schmitt and Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution,* I(II) FLETCHER SECURITY REV. 55 (2014).

[68] Tallinn Manual 2.0, *supra* note 3, r. 15; Articles on State Responsibility, *supra* note 29, art. 4(1).

[69] Tallinn Manual 2.0, *supra* note 3, r. 15; Articles on State Responsibility, *supra* note 29, art. 5.

[70] Tallinn Manual 2.0, *supra* note 3, r. 15, para. 12; Articles on State Responsibility, *supra* note 29, art. 7.

[71] Tallinn Manual 2.0, *supra* note 3, r. 16; Articles on State Responsibility, *supra* note 29, art. 6, para. 1. On the responsibility of a state for an internationally wrongful act associated with an international organization, see Tallinn Manual 2.0, *supra* note 3, r. 31, para. 9. On the responsibility of international organizations, see Int'l Law Comm'n, Draft Articles on the Responsibility of International Organizations, with Commentaries, UN Doc. A/66/10 (2011).

context, however, surrounds the attribution of a non-state actor's cyber operations. Attribution attaches in two circumstances. The first is when a state acknowledges and adopts the operations of the non-state actor as its own.[72] In this relatively unlikely situation, the state not only endorses the non-state actor's cyber operations but also acts to render them the actions of the state itself. Consider a hacker group that is conducting cyber operations against a state. Another state that not only backs the operations, but takes affirmative measures to perpetuate them, either by action or through omission, will bear responsibility for the acts of the group. This possibility was confirmed by the International Court of Justice in the *Tehran Hostages* case, where the government of Iran embraced the acts of the group holding American consular staff hostage and, through actions and omissions, made possible continued detention.[73]

Much more likely is a scenario in which a state "instructs or directs or controls" cyber operations launched by a non-state group or by individuals.[74] Attribution based on instructions differs from the attribution based on empowerment under domestic law in that there is neither a requirement of legal authorization nor a limitation to actions that constitute the exercise of governmental authority. Rather, the state need only instigate the individuals to act on its behalf, for instance as an auxiliary to perform certain cyber operations such as striking particular cyber targets.[75]

This more likely attribution scenario involves a non-state group operating under the direction or control of a state. Although the term "direction or control" is technically disjunctive,[76] direction *and* control are usually expressed ensemble as "effective control."[77] A state is in effective control of the actions of a non-state group when it can exercise the requisite degree of authority over the group's acts, both in terms of engaging in activities or refraining from them. As noted in the commentary to the relevant Article on State Responsibility, a state will only be

---

[72] Tallinn Manual 2.0, *supra* note 3, r.17(b); Articles on State Responsibility, *supra* note 29, art. 11.

[73] United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 74 (May 24).

[74] Tallinn Manual 2.0, *supra* note 3, r.17(a); Articles on State Responsibility, *supra* note 29, art. 8. *See also* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98*, para. 23 (June 24, 2013) [hereinafter 2013 GGE Report]; Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, para. 28(f) (July 22, 2015) [hereinafter 2015 GGE Report].

[75] Tallinn Manual 2.0, *supra* note 3, r.17, para. 4.

[76] Articles on State Responsibility, *supra* note 29, art. 8, para. 7.

[77] Nicaragua, *supra* note 8, ¶ 115; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. and Herz. v. Serb. and Montenegro), 2007 I.C.J. 108, ¶ 400 (Feb. 26) [hereinafter Genocide Case]. *See also* Tallinn Manual 2.0, *supra* note 3, r.17, para. 5; JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 146 (2013). The notion of control in the state responsibility context must not be confused with that of "overall control," which deals with characterization of an armed conflict as "international." Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber judgment, ¶¶ 131–40, 145, 162 (Intl'l Crim. Trib. for the Former Yugoslavia 15 July 1999) [hereinafter Tadic, Appeals Chamber judgment].

responsible on this basis if it "directed or controlled the specific operation and the conduct complained of was an integral part of that operation. The principle does not extend to conduct which was only incidentally or peripherally associated with an operation and which escaped from the State's direction or control."[78] This threshold is not reached when the state simply assists the non-state actor's cyber operations by, for instance, providing financing, malware or training,[79] although such activities themselves may constitute an internationally wrongful act, such as intervention.[80]

2. Breach of Legal Obligation

If the cyber operation is attributable to a state, it must next be asked whether the state is in breach of an international legal obligation. That obligation may be based in either treaty or customary law and may consist of either action or omission. For instance, pursuant to the law of the sea, vessels of one state may pass through the territorial waters of another state in innocent passage so long as they do not engage in activities inconsistent with such passage,[81] such as conducting cyber espionage against the coastal state. Although espionage is not unlawful *per se*,[82] engaging in it during innocent passage is an internationally wrongful act.[83] Thus, if a warship of one state conducts the cyber espionage operations while in the territorial sea of another, those operations are both attributable to the first state—because the warship is a state vessel—and a breach of its obligation to transit territorial waters innocently. The coastal state may respond with countermeasures.

As this example illustrates, cyber operations are subject to rules from many different international law regimes. For instance, many cyber operations involve the use of space assets, thereby implicating space law.[84] Similarly, cyber espionage may implicate the international human right of privacy,[85] while a state's imposition of controls on cyber activities can implicate the right to freedom of expression.[86]

---

[78] Articles on State Responsibility, *supra* note 29, art. 8, para. 3 of commentary.
[79] Nicaragua, *supra* note 8, ¶ 115.
[80] *Id.* at ¶ 242; Tallinn Manual 2.0, *supra* note 3, r. 66.
[81] United Nations Convention on the Law of the Sea, art. 19, Dec. 10, 1982, 1833 U.N.T.S. 3.
[82] Tallinn Manual 2.0, *supra* note 3, r. 32.
[83] *Id.*, r. 48.
[84] *Id.*, ch. 10.
[85] *Id.*, r. 35, para. 6. On the right to privacy, see, e.g., Universal Declaration of Human Rights, art. 12, GA Res. 217A (III), UN Doc. A/810 (Dec. 10, 1948) [hereinafter UDHR]; International Covenant on Civil and Political Rights, art. 17, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc. A/HRC/27/37 (June 30, 2014).
[86] Tallinn Manual 2.0, *supra* note 3, r. 35, paras. 2–4. On the right to freedom of expression, see UDHR, *supra* note 83, art. 19; ICCPR, *supra* note 83, art. 19(2); European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 10, 4 November 1950, 213 U.N.T.S. 222; African Charter on Human and Peoples' Rights, art. 9, June 27, 1981, 21 ILM 58, OAU Doc. CAB/LEG/67/3 rev. 5; American Convention on Human Rights, art. 13, Nov. 22. 1969, 1144 U.N.T.S. 123; Human Rights Committee, General Comment No. 34: Article 19: Freedoms of

However, perhaps the breach most likely to open the door to countermeasures is a violation of the sovereignty of the state in which, or into which, another state's cyber operations are conducted.[87] The International Group of Experts agreed that using cyber means to cause physical damage or injury in another state generally amounts to a breach of that state's sovereignty.[88] It makes no difference whether the injury or damage is the result of targeting public or private cyber infrastructure. The experts likewise agreed that an operation that permanently affects the functionality of cyber infrastructure may constitute a breach of sovereignty,[89] whereas mere espionage, without more, does not.[90] The group could not, however, come to agreement over cyber operations lying between these two extremes. For example, there was no consensus with respect to merely causing cyber infrastructure to operate in a manner in which it was not intended to operate. Similarly, there was disagreement over the mere placement of malware in a system located in another state.[91] However, the experts did concur that a cyber operation interfering with or usurping another state's inherently governmental function, such as law enforcement, is a sovereignty violation irrespective of whether damage or injury results.[92]

3. Conditions on Countermeasures

Because they involve an act that would otherwise be unlawful, countermeasures are subject to strict conditions. Several merit mention. First, countermeasure may not be conducted until the injured state has notified the responsible state that it intends to take countermeasures and gives the responsible state an opportunity to desist in its unlawful conduct.[93] In the cyber context, it is important to point out that the notification requirement is subject to a condition of feasibility, for advance notification that a cyber countermeasure is about to be

---

Opinion and Expression, para. 12, UN Doc. CCPR/C/GC/34 (Sept. 12, 2011); Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, para. 11, UN Doc. A/HRC/29/32 (May 22, 2015).

[87] Tallinn Manual 2.0, *supra* note 3, ch. 1. The classic definition of sovereignty is at Island of Palmas (Neth. v. US) 2 RIAA 829, 838 (Perm. Ct. Arb. 1928). It should be noted that the former General Counsel for the Department of Defense has questioned the status of sovereignty as a primary rule, rather than merely a general principle of international law. U.S. Dep't of Defense, Office of the Gen. Counsel, International Law Framework for Employing Cyber Capabilities in Military Operations (Jan. 19, 2017) (on file with author). This position is contrary to the finding of the International Group of Experts, *see* Tallinn Manual 2.0, *supra* note 3, r. 17; consideration of breaches of sovereignty by the International Court of Justice, *see* Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4 (Apr. 9); and conclusions set forth in other documents prepared in international fora, *see, e.g.*, 2013 GGE Report, *supra* note 70, para 20; 2015 GGE Report, *supra* note 70, paras. 27, 28(b)).

[88] Tallinn Manual 2.0, *supra* note 3, r. 4, paras. 11–13.

[89] *Id*., para. 13.

[90] *Id*., para. 7.

[91] *Id*., para. 14.

[92] *Id*., para. 15–18.

[93] *Id.*, r. 21, paras. 10–11; Articles on State Responsibility, *supra* note 29, art. 52(1). *See also* Gabčíkovo-Nagymaros, *supra* note 52, ¶ 84; Air Services, *supra* note 62, ¶¶ 85–87.

taken may afford the responsible state the opportunity to foil it.[94] Second, countermeasures must be proportionate to the injury to which they respond.[95] In particular, they have to be "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the right question."[96] Third, treaties may contain provisions for the taking of specified remedies in the event of breach. If so, the injured state must resort to them before taking countermeasures.[97]

It is operationally relevant that countermeasures need not be in-kind nor directed at the entity that authored the internationally wrongful act.[98] An injured state may respond with cyber measures, such as cyber operations that violate the sovereignty of the responsible state, to internationally wrongful acts that do not involve cyber, and vice versa. Returning to the law of the sea to illustrate the point, a state that has been targeted by another state's unlawful cyber operations would be entitled to close its territorial sea to vessels of the responsible state transiting in innocent passage. Or consider the case of a state's security organs that conduct unlawful cyber operations against government cyber infrastructure in another state. The injured state would be entitled to respond by directing cyber operations at private corporations in the responsible state, so long as the operations complied with the requirements for countermeasures, such as proportionality.

Of course, a state need not take countermeasures in response to an internationally wrongful act. Responses qualifying as retorsion ("unfriendly" acts that do not violate international law) are always available.[99] The expulsion of diplomats and imposition of economic sanctions following allegations of Russian government hacking intended to interfere with U.S. elections qualified as retorsion.[100] There was therefore no need as a matter of law to establish that the Russian interference in the election amounted to an internationally wrongful act, such as intervention.

Recall that countermeasures may not be taken against anyone other than a responsible state. In certain cases, a state may respond to malicious cyber operations that are not attributable to another state by reference to the obligation

---

[94] Tallinn Manual 2.0, *supra* note 3, r. 21, paras. 11–12; Articles of State Responsibility, *supra* note 29, art. 52(2).
[95] Tallinn Manual 2.0, *supra* note 3, r. 23; Articles on State Responsibility, *supra* note 29, art. 51; Gabčíkovo-Nagymaros, *supra* note 52, ¶ 85; Naulilaa, *supra* note 62, at 1028.
[96] Articles on State Responsibility, *supra* note 29, art. 31.
[97] Tallinn Manual 2.0, *supra* note 3, r. 20, para. 13; Articles on State Responsibility, *supra* note 29, art. 50, para. 10
[98] Tallinn Manual 2.0, *supra* note 3, r. 23, para. 7.
[99] Tallinn Manual 2.0, *supra* note 3, r. 20, para. 4; Articles on State Responsibility, *supra* note 29, *chapeau* to Chapter II of Part 3, para. 3.
[100] The White House, Office of the Press Sec'y, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

of due diligence. Pursuant to that principle, states are obligated to ensure that cyber operations having serious adverse consequences for other states are not mounted from their territory or conducted remotely using cyber infrastructure located therein.[101] The obligation is limited to putting an end to ongoing activities that come to the notice of the territorial state. There is no obligation to take preventive measures to ensure the cyber hygiene of cyber infrastructure located on the state's territory,[102] nor any duty to monitor that infrastructure to identify harmful operations.[103] However, once harmful operations come to the attention of a territorial state—for instance because the target state notifies it of them—the former state must take all reasonable and feasible measures in the circumstances to put an end to the operations.[104] If it fails to do so, it has breached the principle of due diligence and therefore has committed an internationally wrongful act vis-à-vis the target state.

Take the case of harmful cyber operations conducted against one state by a non-state actor operating from another state. A breach of the due diligence obligation by the territorial state would allow the injured state to respond with countermeasures designed to compel the former to put an end to the operations conducted from its territory and thereby come into compliance with its due diligence obligation. Since countermeasures need not be in kind or directed against the author of the internationally wrongful act, the injured state's countermeasures could take the form of cyber operations against the non-state actors. Technically, the "object" of the countermeasures would be the territorial state, not the non-state actors.[105]

Such an action is often compared to the "unwilling and unable" approach to conducting extraterritorial self-defense against non-state actors on the territory of other states discussed above. There is an important difference, however. Countermeasures are only available when the state from which the non-state actors are operating can address the situation but elects not to do so. This is because the obligation is one of conduct, not result.[106] A state that unsuccessfully

---

[101] Tallinn Manual 2.0, *supra* note 3, r. 6. On the principle, see United States v. Arjona, 120, U.S. 479, 483 (1887); S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 88 (Moore, J., dissenting); Island of Palmas, *supra* note 87, at 839; Corfu Channel, *supra* note 87, at 22; UN Secretary-General, Survey of International Law in Relation to the Work of Codification of the International Law Commission, para. 57, UN Doc. A/CN.4/1/Rev.1 (Feb. 1, 1949); Permanent Mission of the Federal Republic of Germany to the United Nations, General Appreciation of the Issues of Information Security, at 4, Note No. 516/2012; 2013 GGE Report, *supra* note 72, paras. 67–68; Nicaragua, *supra* note 8, ¶ 157.

[102] Tallinn Manual 2.0, *supra* note 3, r. 7, paras. 7–8, a conclusion based in part on the International Court of Justice's Genocide judgment, *see* Genocide case, *supra* note 77, at ¶ 431.

[103] Tallinn Manual 2.0, *supra* note 3, r. 7, para. 10.

[104] *Id.*, r. 7.

[105] For the author's explication of the approach, *see* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace,* 125 YALE L.J. F. 68 (2015).

[106] Tallinn Manual 2.0, *supra* note 3, r. 7, para. 24. The state must, however, exhaust all feasible measures at its disposal. Articles on State Responsibility, *supra* note 29, cmt. to art. 12, paras. 11–12; Genocide case, *supra* note 77, at ¶ 430.

attempts to put an end to the cyber operations of the non-state actors, or that makes no attempt to do so because it lacks the technical wherewithal, is not in breach of its due diligence obligation, and accordingly cannot be the object of countermeasures. The state being targeted by the non-state actor's cyber operations would be limited to engaging in law-enforcement.

4. Responses by private entities

The analysis set forth above speaks to responses by states. With the notable exception of self-defense, public international law does not address actions by non-state actors with any granularity. For instance, only cyber operations attributable to states violate the sovereignty of other states. Similarly, the cyber operations of states may violate international law prohibitions on intervention and the use of force, but those of non-state actors do not unless attributable to a state. The latter can violate the domestic law of states enjoying prescriptive jurisdiction,[107] but not international law.

The array of responses provided for in international law with respect to malicious or harmful cyber operations is likewise reserved to states. Private entities enjoy no right under international law to conduct countermeasures or engage in cyber operations pursuant to the right of self-defense. Consider the Sony hack that has been attributed to North Korea.[108] The cyber operation damaged cyber infrastructure, and, because the operation was conducted by a state, violated U.S. sovereignty. Yet the company enjoyed no independent right to hack-back against North Korea. Therefore, any response to the North Korean operations by Sony would have been governed by the domestic law of all states enjoying jurisdiction over that response, the company, the individuals involved, and so forth. Of course, the United States could have employed countermeasures based on North Korea's violation of its sovereignty. Moreover, it could have empowered Sony or another private entity to act on its behalf in responding to the North Korean operations. Had the United States done so, that response would have been attributable to it.

It must be cautioned that if a private entity conducts responsive cyber operations, the state from which those operations are mounted may be obligated, pursuant to the principle of due diligence, to put an end to them. This begs the question of whether the territorial state paradoxically must act to protect another state from private response when the latter has engaged in an internationally wrongful act by directing hostile acts against private entities. The International Group of Experts agreed that the latter state is estopped from asserting a breach of due diligence in these circumstances.[109]

---

[107] Tallinn Manual 2.0, *supra* note 3, r. 8.
[108] For the author's views on the incident, *see* Michael N. 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/.
[109] Tallinn Manual 2.0, *supra* note 3, r. 6, paras. 34–35.

II. The Law of Cyber Warfare

During periods of "armed conflict," the *lex specialis* of international humanitarian law (IHL) applies to operations with a nexus to the conflict in question.[110] Of greatest relevance are those IHL rules related to the "conduct of hostilities," especially the law governing targeting. The analysis that follows tracks the flow of legal logic that applies when considering the legality of an attack under IHL. It begins by assessing when IHL applies and, if so, which aspects thereof do so—the law of international or of non-international armed conflict.

If IHL applies, the weapons employed must be lawful *per se*. Even if lawful in the abstract, though, weapons may only be used lawfully. This requires an assessment of whether the operation in question qualifies as an attack to which the conduct of hostilities rules governing attacks attaches. Such rules include limits on the tactics employed and the targets attacked. Additionally, they require precautions to be taken to minimize harm to civilians and civilian objects and prohibit attacks that are expected to cause harm to them that is excessive relative to the anticipated military advantage likely to accrue from the attack. The discussion that follows considers each of these requirements and prohibitions in the cyber context.

A. *International and Non-International Armed Conflicts*

In any IHL analysis, the first question is whether the situation qualifies as an armed conflict such that the law applicable in such conflicts attaches. When it does not so qualify, peacetime international law, including international human rights law and the other legal regimes set forth earlier, governs cyber operations, as does the domestic law of any state enjoying prescriptive jurisdiction over the matter in question.

There are two forms of armed conflict. An international armed conflict exists whenever hostilities occur between two or more states, or when an organized group that is conducting hostilities against a state is under the overall control of another state.[111] By contrast, a non-international conflict is one between a state and an organized armed group or between organized armed groups.[112]

---

[110] *Id.*, r. 80. On the application of IHL to cyber operations in an armed conflict, *see* UN GGE 2015 Report, *supra* note 74, para. 28(d); The NATO Wales Summit Declaration, *supra* note 10, para. 72; UN Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 2, UN Doc. A/69/112 (June 30, 2014) (Australia); *UN Secretary-General, Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General*, 15, UN Doc. A/68/156 Add. 1 (Sept. 9, 2013) (Japan); Council of the European Union, Conclusions, General Affairs Council Meeting, Doc. 11357/13 (June 21, 2013).

[111] Tallinn Manual 2.0, *supra* note 3 r. 82. The accepted articulation of international armed conflict is Common Article 2 to the 1949 Geneva Conventions. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2, Aug. 12, 1949, 75

Cyber operations that take place during ongoing international or non-international armed conflicts are clearly governed by the IHL applicable in such conflicts. The more difficult question is whether an exchange of cyber operations may alone initiate an armed conflict.[113] Although there is some controversy over the threshold of violence necessary to qualify hostilities as international armed conflict, the better view is that which was proffered in the ICRC commentary to the 1949 Geneva Conventions: "Any difference arising between two States and leading to the intervention of armed forces is an armed conflict . . . It makes no difference how long the conflict lasts or how much slaughter takes place."[114] As to the meaning of hostilities, Tallinn Manual 2.0 describes them as "the collective application means and methods of warfare."[115] The concept is best understood in the cyber context as organized armed forces conducting activities that qualify as cyber "attacks" under IHL, a term that is examined below.

Since cyber "attacks" need not be accompanied by conventional military operations, it is plausible that a cyber-only international armed conflict could occur in the future. It is less likely that a situation involving only cyber operations could amount to a non-international armed conflict. The existence of such conflicts requires that the group involved be "organized" and that the attendant

---

U.N.T.S. 31 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, art. 2, Aug. 12, 1949, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention Relative to the Treatment of Prisoners of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 2, Aug. 12, 1949, 75 U.N.T.S. 287 [hereinafter Geneva IV]. On qualification as an international armed conflict based on a state's "overall control" of an organized armed group, *see* Tadic, Appeals Chamber judgment, *supra* note 77, ¶¶ 131–40, 145, 162.

[112] Tallinn Manual 2.0, *supra* note 3, r. 83. The accepted articulation of non-international armed conflict is Common Article 3 to the 1949 Geneva Conventions. Geneva Conventions I–IV, *supra* note 111, art. 3. *See also* Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶¶ 67, 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) [hereinafter Tadic, Interlocutory Appeal].

[113] The author's views on the subject are set forth in Michael N. Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT AND SECURITY L. 245 (2012).

[114] INT'L COMMITTEE OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD, para. 236 (2016) [hereinafter 2016 GC I Commentary]; INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD 32 (Jean Pictet ed., 1952); INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED, SICK, AND SHIPWRECKED MEMBERS OF THE ARMED FORCES AT SEA 28 (Jean Pictet ed., 1960); INT'L COMM. OF THE RED CROSS, COMMENTARY: RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960); INT'L COMM. OF THE RED CROSS, COMMENTARY: GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 20 (Jean Pictet ed., 1958). *See also* Tadić, Interlocutory Appeal, *supra* note 110, ¶ 70; DoD Manual, *supra* note 10, para. 3.4.2.

[115] Tallinn Manual 2.0, *supra* note 3, r. 82, para. 11.

violence reach a high level of intensity.[116] The requirement of organization excludes cyber operations mounted by small groups or individuals who are not operating in concert, even though they might be targeting the same entities. That of intensity necessitates cyber operations that are highly destructive or lethal. Although the level is ill-defined in IHL, it certainly exceeds the intensity of violence during civil disturbances, riots, and the like.[117] Merely causing injuries, or even some deaths, would not cross the threshold. Given these criteria, the prospect of a "cyber-only" non-international armed conflict is low.

An additional factor bearing on the international law governing cyber operations is the geography of the armed conflict.[118] During an international armed conflict, cyber operations from, to, or affecting neutral states are, in addition to IHL, subject to the law of neutrality, a topic addressed below. With respect to non-international armed conflict, the applicability of IHL beyond the territory of the state involved is in dispute.[119] By one view, IHL applies to such operations wherever they occur, for the existence of the armed conflict, as mentioned above, is based on the status of the actors involved and factors such as organization and intensity, rather than geography.[120] By a second view, IHL only applies to operations in the territory of the state and border areas into which the hostilities "spill over."[121] The debate has unique relevance in the cyber context because most cyber operations during an armed conflict do not rely, as kinetic operations usually do, on geographical positioning.

Whether cyber operations are conducted during an international or non-international armed conflict, the conduct of hostilities analysis is similar. Additional Protocol I to the 1949 Geneva Conventions, which applies for states parties in an international armed conflict, sets forth many of the applicable

---

[116] *Id.*, r. 83, para. 6; Tadić, Interlocutory Appeal, *supra* note 112, ¶ 70; Prosecutor v. Milošević, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, ¶¶ 16–17 (Int'l Crim. Trib. for the Former Yugoslavia June 16, 2004); Prosecutor v. Anto Furundžija, Case No. IT-95-17-T, Trial Chamber Judgment, ¶ 59 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998); Prosecutor v. Delalić/Mucić, Case No. IT-96-21-T, Trial Chamber Judgment, ¶ 183 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998); 2016 GC I Commentary, *supra* note 114, para. 421. On intensity, see especially Prosecutor v. Haradinaj, Case No. IT-04-84-T, Trial Chamber Judgment, ¶ 40–49 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 3, 2008); Prosecutor v. Lubanga, ICC-01/04-01/06, Trial Chamber Judgment, ¶ 538 (Mar. 14, 2012).

[117] Tallinn Manual 2.0, *supra* note 3, r. 83, para. 5; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, art. 1(2), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]; Statute of the International Criminal Court, art. 8(f), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute].

[118] Tallinn Manual 2.0, *supra* note 3, r. 81.

[119] For the author's view on the matter, *see* Michael N. Schmitt, *Charting the Legal Geography of Non-International Armed Conflict*, 90 INT'L L. STUD. 1 (2014).

[120] Harold Hongju Koh, Address at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law (Mar. 25, 2010).

[121] 32nd Int'l Conference of the Red Cross and Red Crescent, *International Humanitarian law and the Challenges of Contemporary Armed Conflicts* (Dec. 8–10, 2015), at 18–19 [hereinafter Challenges Report]; 2016 GC I Commentary, *supra* note 114, paras. 465–82.

rules.[122] Although treaty based, the Additional Protocol I rules cited below, except as otherwise indicated, generally reflect customary international law applicable in both international and non-international armed conflicts.

B. *Weapon Reviews*

The "means of warfare," or weapons, used in the conduct of hostilities are required to be lawful *per se* based on their intended use—that is, lawful regardless of how they are actually used in combat.[123] Therefore, states are obliged to take steps to ensure that their weapons comply with IHL before they are fielded or used.[124] This weapon review requirement applies fully to cyber weapons.[125] *Tallinn Manual 2.0* defines such weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack."[126] The definition of "attack" in the context of cyber operations is discussed below.

It is important to note that cyber weapons can be developed during the armed conflict, including by fielded units, to exploit vulnerabilities that have been just identified or to take advantage of a situation that has presented itself in the battlespace. The weapons review requirement applies equally in these circumstances. However, because there is no set methodology by which the review must be conducted, the International Group of Experts agreed that this requirement may be satisfied by an assigned legal officer providing his or her evaluation to the commander considering the cyber weapon's employment.[127]

As it is a customary law rule, all states must conduct a weapons review of cyber weapons prior to acquisition or use. States Parties to Additional Protocol I are further required in the study, development, acquisition or adoption of both cyber means and "methods" (how a weapon is intended to be employed) of warfare to assess whether its employment will comply with any international law rules binding on the respective state.[128]

---

[122] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

[123] This obligation derives from the general requirement that states must conduct their operations in accordance with international humanitarian law. Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, art. 1, Oct. 18, 1907, 36 Stat. 2277 [hereinafter Hague Regulations]; Geneva Conventions I–IV, *supra* note 111, common art. 1.

[124] Additional Protocol I, *supra* note 122, art. 36.

[125] Tallinn Manual, *supra* note 3, r. 110. *See also* DoD Manual, *supra* note 10, para. 16.6.

[126] Tallinn Manual, *supra* note 3, r. 103, para. 2. On the definition of a "cyber attack" under IHL, see *id.*, r. 92.

[127] *Id.*, r. 110, paras. 9–10.

[128] *Id.*, r. 110(b); Additional Protocol I, *supra* note 122, art. 36.

Cyber weapons and tactics that are designed, or of a nature, to cause superfluous injury or unnecessary suffering are unlawful *per se*.[129] Such weapons and tactics needlessly aggravate the suffering of combatants, members of organized armed groups, or civilian direct participants in the hostilities (see below) without providing the attacker any further military advantage. Historic examples include glass-filled projectiles and knives with serrated edges. It is difficult to imagine a cyber weapon running afoul of this prohibition.

Much more likely to render a cyber weapon unlawful is the prohibition on methods or means of warfare that cannot be directed at specific military objectives,[130] or that have effects that cannot be limited as IHL requires,[131] and therefore are susceptible to striking military objectives and civilians or civilian objects without distinction. Examples include malware devised for introduction into shared networks that is programmed to exploit a vulnerability found in both civilian and military systems, when it would have been possible to limit its operation to military systems, and malware designed for embedding in online websites that are likely to be accessed by both civilian and military personnel (so long as the resulting consequences rise to the level of an "attack").

Lest this prohibition be overstated, it is important to emphasize that if a cyber weapon is capable of distinction in the environment in which it is intended to be used, it is lawful *per se* and the question becomes whether it was used lawfully once employed. For instance, the spread of a specific type of malware may be difficult to control, but if the malware is meant for use in closed military networks it would present no obstacle with respect to the weapons review. Should it subsequently be used in an indiscriminate fashion, the use would, as will be explained, be unlawful.

C. *Meaning of the Term "Attack"*

Once it is determined that the proposed cyber weapon and, for states Parties to Additional Protocol I, method of cyber warfare is lawful, it is necessary to determine whether the planned cyber operation qualifies as an "attack" under IHL.[132] This is because most rules dealing with the conduct of hostilities are expressed in terms of attacks; it is prohibited to "attack" civilians and civilian objects, "attacks" that are disproportionate are forbidden, feasible precautions must be taken during an "attack" to avoid harm to civilians and civilian objects,

---

[129] Tallinn Manual, *supra* note 3, r. 104; Hague Regulations, *supra* note 123, art. 23(e); Additional Protocol I, *supra* note 122, art. 35(2). *See also* Rome Statute, *supra* note 117, art. 8(2)(b)(xx); Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, pmbl., Apr. 10, 1981, 1342 U.N.T.S. 137; Convention on the Prohibition on the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, pmbl., Dec. 3, 1997, 2056 U.N.T.S. 211.

[130] Tallinn Manual, *supra* note 3, r.105(a); Additional Protocol I, *supra* note 122, art. 51(4)(b).

[131] Tallinn Manual, *supra* note 3, r.105(b); Additional Protocol I, *supra* note 122, art, 51(4)(c).

[132] Tallinn Manual 2.0, *supra* note 3, r. 92. Additional Protocol I, *supra* note 122, art. 49(1).

and so forth (see below). If a cyber operation does not qualify as an attack, rules containing the term do not attach. For example, it is lawful to direct cyber operations at civilian cyber infrastructure so long as they do not qualify as attacks, and no other prohibitory IHL rule applies. The classic case is a psychological operation employing social media to undercut civilian support for the enemy government and its war effort.[133]

It is essential to distinguish the term "attack," which is an IHL term of art, from "armed attack," which, as discussed, applies in the *jus ad bellum* context and is the condition precedent for a state to act in national self-defense. The discussion that follows deals solely with attacks in the IHL sense.

The definition of the term "attack" remains unsettled among IHL experts, including members of the International Group of Experts.[134] Nevertheless, common ground exists. It is well accepted that a cyber operation resulting in physical damage to objects or injury or death of individuals qualifies.[135] This is so irrespective of whether the requisite harm is caused to the target of the operation or occurs as collateral damage to civilians or civilian objects. To illustrate, a cyber operation that damages cyber infrastructure or the systems that rely upon it, as in causing machinery to operate in a manner that causes it to break apart, is an attack; if the infrastructure or machinery is civilian in character, the operation would amount to an unlawful attack on a civilian object.

A majority of the International Group of Experts also took the position that the loss of cyber infrastructure's functionality equates to damage for the purpose of defining the term attack.[136] This so-called "functionality test" encompasses cyber operations that render cyber infrastructure permanently inoperative or that necessitate significant repair within the ambit of the term "attack."[137]

---

[133] *See, e.g.*, Bryan Lee, *The Impact of Cyber Capabilities in the Syrian Civil War*, SMALL WARS J. (Apr. 26, 2016), http://smallwarsjournal.com/jrnl/art/the-impact-of-cyber-capabilities-in-the-syrian-civil-war.

[134] Tallinn Manual 2.0, *supra* note 3, r. 92, para. 13. On the author's views, see Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack,* 96 INT'L REV. RED CROSS 189 (2014). *See also* Challenges Report, *supra* note 121, at 41–42.

[135] Tallinn Manual 2.0, *supra* note 3, r. 92, para. 4.

[136] *Id*., r. 92, para. 10–11.

[137] For instance, consider the 2015 cyber operations against Ukrainian electrical generation cyber infrastructure during the on-going international armed conflict between Russia and Ukraine. Although there may be issues as to attribution, as well as whether the electrical grid concerned was a lawful military objective, the fact that some components of the system were rendered permanently inoperable qualifies the operations as an attack. *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

It should be cautioned in this regard that there is a lack of consensus as to consequences falling below this level.[138] For instance, the International Group of Experts could not agree about cyber operations that necessitate reloading the operating system or that delete, corrupt, or alter data that is necessary for purpose-built cyber infrastructure to perform its intended function. It did agree, however, that temporary denial of service operations causing only inconvenience or irritation do not constitute attacks and accordingly are not subject to the conduct of hostilities rules specifically governing attacks.[139] The ICRC has correctly observed, for instance, that "the jamming of radio communications or television broadcasts has not traditionally been considered an attack in the sense of IHL."[140] There is no reason to conclude that achieving the same results by cyber means should be treated differently.

A cyber operation directed against cyber infrastructure that causes no damage or injury to the system itself is nevertheless an attack if it is reasonably foreseeable that the attack will indirectly cause damage or injury.[141] The paradigmatic example of this kind of indirect damage is a cyber operation against a dam's SCADA system that triggers a release of waters to deny the enemy use of the flooded area. If individuals downstream drown and property is destroyed, the operation amounts to an attack even though the dam has suffered no damage. Since the operation is an attack, the rule of proportionality (discussed below), for instance, would be highly relevant in assessing its lawfulness.

Cyber operations that do not qualify as attacks may nevertheless be unlawful or subject to limitations when the intended target is subject to special protection. Such protection extends to, *inter alia*, medical, religious, humanitarian assistance, civil defense, and United Nations personnel, property, and activities; detained persons, the wounded and sick, children, and journalists; and cultural objects, installations containing dangerous forces, objects indispensable to the civilian population, and the environment.[142] Certain special protections are

---

[138] In deconstructing the debate over the functionality test, the ICRC has usefully catalogued the differing views: "One view is to consider that cyber attacks are only those operations that cause violence to persons or physical damage to objects. A second approach is to make the analysis dependent on the action necessary to restore the functionality of the object, network or system. A third approach is to focus on the effects that the operation has on the functionality of the object." Challenges Report, *supra* note 121, at 41–42. The author agrees with the ICRC that "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" because "an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities." *Id*. at 41.

[139] Tallinn Manual 2.0, *supra* note 3, r. 92, para. 14.

[140] Challenges Report, *supra* note 121, at 42.

[141] Tallinn Manual 2.0, *supra* note 3, r. 92, para. 15.

[142] *Id.*, ch. 18. These rules are set forth in various instruments, including: Hague Regulations, *supra* note 123, Geneva Conventions I–IV, *supra* note 111, Additional Protocol I, *supra* note 122; Additional Protocol II, *supra* note 117, Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, May 25, 2000, 2173 U.N.T.S. 222; Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict with

customary in nature and therefore apply to all states.[143] Others, such as that regarding installations containing dangerous forces,[144] are treaty-based and bind only states Parties to the respective instruments.

D. *Targets*

Once it is determined that a cyber operation qualifies as an attack, the target itself must be considered. The fulcrum upon which the law of targeting rests is the principle of distinction.[145] This customary law principle, reflected in article 48 of Additional Protocol I, provides: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[146] By the principle, cyber attacks may directly target, as will be explained, only military objectives, combatants, members of organized armed groups, and civilians directly participating in hostilities.

1. Objects as targets

The first category of targetable persons and objects, military objectives, consists of "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military of advantage."[147] Objects that do not satisfy the definition are civilian objects and, as such, are protected from direct attack.[148]

Regulations for the Execution of the Convention, May 14, 1954, 249 U.N.T.S. 240; Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), Dec. 10, 1976, 1108 U.N.T.S. 151; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, Mar. 26, 1999, 2253 U.N.T.S. 212.

[143] *See* 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW STUDY 59–158 (Int'l Comm. of the Red Cross, 2005) [hereinafter Customary IHL Study].

[144] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 140; Additional Protocol I, *supra* note 122, art. 54(2).

[145] The principle finds its genesis in the 1868 St Petersburg Declaration, which provides that "the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy." Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 29 Nov./11 Dec. 1868, *reprinted in* 18 AM. J. INT'L L. SUPPLEMENT: OFFICIAL DOCUMENTS 95 (1907).

[146] Additional Protocol I, *supra* note 122, art. 48; *see also* Tallinn manual 2.0, *supra* note 3, r. 93. Customary IHL Study, *supra* note 143, rr. 1, 7. The reference in article 48 to "military objectives" is meant to encompass persons and objects that may be lawfully targeted. *See* Jean S. Pictet et al., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, para. 1874 (International Committee of the Red Cross, 1987) [hereinafter Additional Protocols Commentary]. The International Court of Justice has labeled distinction a "cardinal principle" of IHL. Nuclear Weapons, *supra* note 8, ¶ 78.

[147] Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 52(2). This definition was adopted in Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100 and

Military objectives by nature are those objects that are military in character, such as command-and-control facilities, communications equipment, radar sites, and the like.[149] Civilian objects become military objectives by "use" when the enemy uses them for military ends.[150] As an example, if the military relies in part on a civilian electrical grid or telephone system, those entities become military objectives for as long as they are so used. The term "purpose" refers to future use.[151] For instance, if reliable intelligence is acquired that civilian communication systems are going to be used to provide redundancy for military systems, the former become military objectives by purpose even before being converted to that use. Finally, "location" refers to an area that has become militarily significant.[152] In the dam example above, the downstream territory that is flooded qualifies as a military objective on this basis.

A point of controversy of heightened relevance in the cyber context involves so-called "war-sustaining objects.[153] It is widely accepted that "war-fighting" and "war-supporting" objects are lawful targets. Warfighting objects are those used to engage in the hostilities, such as military cyber infrastructure. War-supporting objects directly contribute to the hostilities, although they not used during them. Factories producing military equipment are the paradigmatic example and accordingly may lawfully be targeted by cyber means.

"War-sustaining" objects only indirectly support the war effort. An example would be an industry that provides significant revenue upon which the armed conflict depends. This is most likely to be the case in situations where a state depends on proceeds or taxes from the industry to fund the war effort, as in the case of oil for many oil-exporting states. As an example, cyber infrastructure that controls oil storage facilities or a pipeline used for the transshipment of oil is, by the war-sustaining approach, a lawful military objectives. The United States takes the position that war-sustaining objects are valid targets that may be directly attacked.[154] A majority of the International Group of Experts rejected the

---

appears in many military manuals, including that of the United States. DoD Manual, *supra* note 10, para. 5.6.3. As to its customary nature, see Customary IHL Study, *supra* note 143, r. 8.

[148] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 99; Additional Protocol I, *supra* note **Error! Bookmark not defined.**, art. 52(1). Customary IHL Study, *supra* note 143, r. 7.

[149] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100, para. 8. Additional Protocols Commentary, *supra* note 146, para. 2020.

[150] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100, para. 10; Hague Regulations, *supra* note **Error! Bookmark not defined.**, art. 27; Additional Protocols Commentary, *supra* note 146, para. 2022.

[151] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100, para. 12; Additional Protocols Commentary, *supra* note 146, para. 2022.

[152] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100, para. 9; Additional Protocols Commentary, *supra* note 146, para. 2021.

[153] Tallinn Manual 2.0, *supra* note **Error! Bookmark not defined.**, r. 100, paras. 18–19.

[154] DoD Manual, *supra* note 10, para. 5.6.6.2. *See also* Brian Egan, *International Law, Legal Diplomacy, and the Counter-ISIL Campaign*, 92 INT'L L. STUD. 235, 242 (2016).

approach on the basis that the connection between such objects and military operations is too attenuated to produce a "definite military advantage."[155]

A controversy specific to the cyber operations is the legal nature of data.[156] When a cyber operation destroys, alters, or manipulates data in a fashion that directly leads to physical damage or injury, it qualifies as an attack and is therefore subject to the prohibition on attacking civilian objects. However, disagreement exists regarding whether the data itself qualifies as an object, such that the prohibition on attacking civilian objects applies to it.

Within the International Group of Experts, the majority view was that data is intangible and consequently not an object. In the assessment of these Experts, the fact that a cyber operation destroys or alters data does not alone qualify that operation as an attack and, if the data concerned is civilian in nature, thereby render the operation unlawful.[157] These experts pointed out that treating data as an object would be overbroad in the sense that it would rule out many common cyber operations that are engaged in during armed conflict in order to affect civilian systems. For example, most psychological operations mounted by cyber means against civilian information systems would be prohibited. Yet, such a prohibition would run counter to state practice and the understanding of most states that employ, or plan on employing, cyber operations during armed conflicts. A minority of the experts countered that failing to consider data as an object would, as a matter of law, allow a belligerent to conduct highly disruptive (albeit not physically harmful) operations against the civilian population.[158] To illustrate, the interpretation would allow cyber operations that destroy data bases used for educational purposes or contain important state pension data.

There is merit in both views. Failure to treat data as an object is under inclusive in terms of the protective object and purpose of IHL, whereas doing so is over inclusive in the sense that it runs counter to the notion of military necessity recognized by that body of law. A possible resolution to this predicament would be to recognize that certain "essential civilian functions" rely upon data and merit special protection under IHL.[159] However, such protection is, in the current state of the law, *lex ferenda*, not *lex lata*.

---

[155] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, r. 100, para. 19.

[156] The author's views on the matter are set forth in Michael N. Schmitt, *The Notion of 'Objects" during Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 ISR. L. REV. 81 (2015).

[157] Tallinn Manual, *supra* note **Error! Bookmark not defined.**, r. 100, para. 6. The majority relied, in part, on the description of an object as something "visible and tangible" in the Additional Protocols Commentary *supra* note 146, paras. 2007–08.

[158] Tallinn Manual 2.0, *supra* note 3, r. 100, para. 7.

[159] The author proposed this approach in Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 296 (2014). The ICRC appears to support the same approach. *See* Challenges Report, *supra* note 121, at 43.

Finally, the issue of dual-use objects looms large in the cyber context. A dual-use object is one that is used for both military and civilian purposes, such as submarine communications cables carrying both military and civilian traffic, a server farm that stores both civilian and military data, or social media that is used to pass intelligence or organize operations. Under IHL, a civilian object becomes a military objective when used for military purposes, no matter how slight that use. They may be directly targeted, albeit subject to other IHL provisions such as the rule of proportionality and the requirement to take precautions in attack.[160]

2. Persons as targets

The "object" of a cyber attack is usually cyber infrastructure, rather than individuals. Nevertheless, IHL is clear. A cyber operation targeting cyber infrastructure that is intended to cause injury to or death of individuals is an attack on those individuals. If those individuals are civilians, the attack is unlawful.

Three broad categories of individuals are subject to direct cyber attack under IHL[161]; all others are civilians (or specially protected members of the military, like religious and medical personnel and those who are *hors de combat*[162]) who enjoy legal protection from direct attack.[163] The first category consists of "combatants" during an international armed conflict, a term that includes members of the regular armed forces of a party to the conflict and members of militias or volunteer corps forming part of such armed forces. It also encompasses militias and other volunteer corps, including organized resistance movements, that belong to a party, are commanded by a person responsible for his or her subordinates, wear a distinctive emblem or attire recognizable at distance, carry arms openly, and conduct operations in accordance with IHL.[164]

The second category comprises members of an organized armed group during either an international or non-international armed conflict. The group need not be recognizable by a distinctive emblem, carry arms openly, or conduct their operations in accordance with IHL to qualify as an organized armed group. Although its members do not benefit from belligerent immunity or acquire prisoner of war status if captured, as combatants do, they are generally treated like combatants with respect to targeting rules.[165] Thus, it is lawful to conduct cyber

---

[160] Tallinn Manual 2.0, *supra* note 3, r. 101.

[161] *Id.*, r. 96. Note that members of a *levée en masse* are also targetable. *Id.* at rr. 88, 96(d).

[162] Tallinn Manual 2.0, *supra* note 3, r. 86, para. 3. Geneva Convention I, *supra* note 111, arts. 24–25; Additional Protocol I, *supra* note 122, art. 41.

[163] Tallinn Manual 2.0, *supra* note 3, r. 94; Additional Protocol I, *supra* note 122, art. 51(2); Additional Protocol II, *supra* note 117, art. 13(2); Customary IHL Study, *supra* note 143, r. 1.

[164] Tallinn Manual, *supra* note 3, r. 87, paras. 4, 5, 96(a); Hague Regulations, *supra* note 123, art. 1; Geneva Convention III, *supra* note 111, art. 4A(1) & (2). Although Geneva Convention III deals with prisoner of war status, it is generally understood as accurately denoting combatants for targeting purposes.

[165] Tallinn Manual 2.0, *supra* note 3, r. 96(b). The concept of an organized armed group in the targeting context was first developed in a comprehensive manner in INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES

attacks meant to kill or injure members of organized armed groups, including those members who are engaged in cyber activities. A group of organized hackers operating collaboratively who are conducting operations at the "attack" level likewise qualify as an organized armed group. As the notion of combatancy does not extend to non-international armed conflict, fighting forces in such conflicts are organized armed groups.

Although there is consensus that members of organized groups are subject to cyber attack, disagreement exists as to who constitutes a member for this purpose.[166] Some members of the International Group of Experts suggested, as does the ICRC, that only those members having a "continuous combat function" may be targeted at any time.[167] A continuous combat function is a position within the group that involves activities designed to negatively affect enemy operations.[168] For instance, group members who are engaged in cyber operations against enemy forces would so qualify. Those who do not have a continuous combat function, such as individuals responsible solely for administrative functions, would become directly targetable only if they directly participate in the hostilities (see below).

The other experts rejected the "continuous combat function" approach and took the view that membership in the group alone suffices to render an individual targetable at any time.[169] They pointed out that because combatants are always targetable irrespective of the function they serve in the armed forces, it would create a pernicious imbalance to treat their opponents, who enjoy no "right" to engage in hostilities in the first place, more favorably with respect to targetability.[170]

The final category of targetable persons comprises individuals who are neither combatants nor members of an organized armed group, but nevertheless directly participate in the hostilities in an *ad hoc* or spontaneous fashion.[171] In the cyber context, it would include, for instance, individual hackers targeting military cyber infrastructure, multiple hackers who are directing operations against common cyber infrastructure but are not acting collaboratively, and persons who collect intelligence by cyber means, identify cyber vulnerabilities, or develop exploits that they pass on to a party to the conflict. Direct participants in

---

UNDER INTERNATIONAL HUMANITARIAN LAW (Nils Melzer ed., 2009) [hereinafter Interpretive Guidance].

[166] Tallinn Manual 2.0, *supra* note 3, r. 96, para. 4.

[167] Interpretive Guidance, *supra* note 165, at 27.

[168] *Id*. at 33. The individual would be classified as a direct participant in hostilities (see below) but for membership in the group.

[169] Tallinn Manual 2.0, *supra* note 3, r. 96, para. 4.

[170] Additional Protocol I, *supra* note 122, art. 43(2). The author agrees. *See* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT'L SEC. J. 5 (2010).

[171] Tallinn Manual 2.0, *supra* note 3, rr. 96(c), 97; Additional Protocol I, *supra* note 122, art. 51(3); Additional Protocol II, *supra* note 117, art. 13(3); Customary IHL Study, *supra* note 143, r. 6.

hostilities may be attacked for such time as they so participate and do not factor into the proportionality analysis or need to be considered with respect to the taking of precautions in the attack (see below).[172]

To qualify as direct participation, the act in question must satisfy three constitutive elements.[173] First, the individual must be engaging in an activity that negatively affects, or is intended to negatively affect, an adversary's military operations or capabilities, or that causes injury to civilians or destruction of civilian objects. Note that there is no requirement that the cyber operation be physically destructive or injurious. For example, a denial of service operation directed at enemy military cyber infrastructure would suffice. Second, the act must be the direct cause of the harm intended. Consider the case of an individual who designs malware and makes it available on-line. The malware is subsequently acquired by the enemy and used for cyber attacks. In this case, causation is too attenuated to constitute direct participation on the part of the malware designer. However, developing custom-made malware to exploit a specific enemy vulnerability would amount to direct participation. Finally, the act in question must have a belligerent nexus, that is, it must be related to the conflict. Cyber crime made possible by the fact that the conflict has hindered a state's ability to conduct law enforcement activities, for instance, would lack the requisite nexus. Although the criminality would not have been possible but for the armed conflict, it has been engaged in for purely personal reasons.

Unlike combatants and members of organized armed groups, direct participants may only be attacked for such time as they so participate.[174] This limitation has taken on added significance in the cyber context. Some members of the International Group of Experts agreed with the ICRC that the "for such time" widow means an individual may only be attacked during his or her act of participation, while engaged in preparatory measures immediately preceding the act, or when deploying to or returning from engaging in it.[175] Other experts countered that this approach could severely limit the ability to target direct participants engaged in cyber operations because such operations may involve little immediate preparation, require no deployment, and occur near instantaneously. They opined that the "for such time" limitation should be interpreted as including the period between the individual's initial cyber operation and the point at which he or she decides to desist altogether from further participation.[176] Take the individual who conducts attacks once or twice a week over a period of several months. By the latter approach, that individual would be targetable by either cyber or kinetic means throughout that period.

---

[172] Tallinn Manual 2.0, *supra* note 3, r. 97, para. 3.
[173] *Id*. at r. 97, paras. 5–7; Interpretive Guidance, *supra* note 165, at 46.
[174] Tallinn Manual 2.0, *supra* note 3, r. 97, para. 8. The "for such time" limitation appears in the text of the relevant law. *See* Additional Protocol I, *supra* note 122, art. 51(3); Additional Protocol II, *supra* note 117, art. 13(3).
[175] Interpretive Guidance, *supra* note 165, at 70–73.
[176] Tallinn Manual 2.0, *supra* note 3, r. 97, para. 8. *See also* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 177 (2016).

3. Doubt

As explained, objects or persons that do not qualify as, respectively, a military objective or directly targetable individuals, are civilian as a matter of law and may not be directly attacked. Controversy exists over situations in which the status of a person or object is in doubt. Although it has been asserted that no presumption of civilian status exists in such cases,[177] the International Group of Experts concurred that a presumption of civilian status attaches whenever the degree of doubt, considering the attendant circumstances, is such that a reasonable commander or other responsible official would hesitate to attack. The presumption applies to persons generally[178] and to "objects 'normally dedicated to civilian purposes' and any cyber infrastructure upon which they rely."[179]

4. Reprisals

In very limited circumstances, cyber attacks against prohibited targets may be permissible as a form of belligerent reprisal.[180] Reprisals are unlawful actions taken in response to the enemy's unlawful actions that are intended to cause the enemy to desist in its unlawful conduct. That is their sole purpose; retaliation is forbidden.[181] There are significant limitations and restrictions on the taking of reprisals. For example, cyber reprisals against prisoners of war, interned civilians, those who are *hors de combat*, civilians in occupied territory or otherwise under the control of an adverse party to the conflict, and medical personnel, facilities, vehicles, and equipment are prohibited.[182] Additionally, states party to Additional Protocol I may not take reprisals against civilians or an assortment of specified objects, including civilian objects such as civilian cyber infrastructure.[183]

---

[177] The DoD Manual provision on the subject takes the position that presumptions of civilian status are binding only on Parties to Additional Protocol I and that no such presumption appears in customary international law. DoD Manual, *supra* note 10, para. 5.4.3.2.

[178] Tallinn Manual 2.0, *supra* note 3, r. 95; Additional Protocol I, *supra* note 122, art. 50(1); Customary IHL Study, *supra* note 143, commentary accompanying r. 6.

[179] Tallinn Manual 2.0, *supra* note 3, r. 102; Additional Protocol I, *supra* note 122, art. 52(3); Customary IHL Study, *supra* note 143, commentary accompanying r. 10.

[180] Tallinn Manual 2.0, *supra* note 3, r. 108. There is no legal concept of belligerent reprisals in non-international armed conflict. *See* Customary IHL Study, *supra* note 143, r. 148; 2016 GC I Commentary, *supra* note 114, paras. 904–905.

[181] FRITS KALSHOVEN, BELLIGERENT REPRISALS 33 (2005).

[182] Geneva Convention I, *supra* note 111, art. 46; Geneva Convention II, *supra* note 111, art. 47; Geneva Convention III, *supra* note 111, art. 13; Geneva Convention IV, *supra* note 111, art. 33; Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, art. 3, Oct. 10, 1980, 1342 U.N.T.S. 168 [hereinafter Mines Protocol]; Customary IHL Study, *supra* note 143, r. 146. On the conditions for the taking of reprisals, see Customary IHL Study, *supra* note 143, r. 145 and commentary accompanying r. 145.

[183] *See* Tallinn Manual 2.0, *supra* note 3, r. 109; Additional Protocol I, *supra* note 122, arts. 20, 51(6), 52(1), 53(c), 54(4), 55(2), 56(4); *see also* Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be

E. *Tactics*

After determining that the target is a lawful one, it is necessary to assess the tactics to be employed. Among the tactics that are prohibited, two deserve particular attention. First, it is prohibited to conduct indiscriminate cyber attacks. An indiscriminate attack is one that is either not directed at a specific lawful target or directed at a lawful target without the effects of the attack, in the attendant circumstances, being controlled.[184] Treating clearly separated and distinct military objectives located in a concentration of civilian objects as a single military objective is likewise indiscriminate.[185] Examples of the three would be, respectively, launching cyber attacks while making no attempt to direct them at particular cyber infrastructure qualifying as a military objective, launching malware designed for use against a closed military network into a military network connected to civilian systems, and attacking cyber infrastructure used for military and civilian purposes when it would be feasible to target only the military aspects thereof.

The second key tactic prohibited by IHL is engaging in perfidy by cyber means.[186] Perfidy is the killing or injuring of an adversary by engaging in actions "that invite the confidence of an adversary to lead him to believe he is entitled to, or is obliged to accord, protection under [IHL] with intent to betray that confidence."[187] For Parties to Additional Protocol I, perfidious conduct resulting in capture is also prohibited.[188]

To constitute perfidy, the act must involve feigning protected status under IHL to trick the enemy. A party to the conflict, for example, might send an email purporting to be from the ICRC that supposedly arranges for the visit of detainees. The expectation of the visit is then exploited by the sender's force to acquire access to the installation and conduct attacks therein. Perfidy must be distinguished from ruses, which are lawful and merely intended to mislead the enemy or cause it to act recklessly.[189] Examples include transmitting false orders

---

Excessively Injurious or to Have Indiscriminate Effects, art. 37, 2048 U.N.T.S. 133 (as amended May 3, 1996) [hereinafter Amended Mines Protocol]; Mines Protocol, *supra* note 182, art. 3(2). For an example of how a state Party to Additional Protocol I has limited the effect of these provisions, *see* U.K. Statement made upon Ratification of Additional Protocols I and II, para. (m), *in* DOCUMENTS ON THE LAW OF WAR 510 (Adam Roberts and Richard Guelff eds., 3rd ed., 2000).

[184] Tallinn Manual 2.0, *supra* note 3, r. 102; Additional Protocol I, *supra* note 122, art. 51(4)(b) and (c); Customary IHL Study, *supra* note 143, rr. 12, 71.

[185] Tallinn Manual 2.0, *supra* note 3, r. 112; Additional Protocol I, *supra* note 122, art. 51(5)(a); Customary IHL Study, *supra* note 143, r. 13.

[186] Tallinn Manual 2.0, *supra* note 3, r. 122; Hague Regulations, *supra* note 123, art. 23(b); Customary IHL Study, *supra* note 143, r. 65.

[187] Tallinn Manual 2.0, *supra* note 3, r. 122. *See also* text of Additional Protocol I, *supra* note 122, art. 37(1).

[188] Additional Protocol I, *supra* note 122, art. 37(1).

[189] Tallinn Manual 2.0, *supra* note 3, r. 123; Additional Protocol I, *supra* note 122, art. 37(2); Customary IHL Study, *supra* note 143, r. 57.

to the enemy, creating dummy computer systems to simulate nonexistent forces, and using honeynets or honeypots designed to lure the enemy into a cyber trap.[190] Perfidy must also be distinguished from the misuse during cyber operations of protective emblems, a prohibition that, unlike perfidy, requires no particular result in order to be violated.[191] For instance, sending emails containing the ICRC's Red Cross, Red Crescent, or Red Crystal, or another recognized protective emblem, is unlawful irrespective of whether the intent is to betray the enemy's confidence in order to conduct an attack.

F. *Precautions in Attack*

Even when the cyber weapon to be used is lawful, the target is subject to lawful cyber attack, and no forbidden tactics will be employed, an attacker must take precautions to minimize harm to civilians and civilian objects, so long as doing so does not sacrifice military advantage.[192] This obligation requires an attacker to do everything feasible to verify that the target is a military objective, choose the methods or means of warfare and the target that will minimize or avoid collateral damage, and cancel or suspend an attack should it becomes apparent that the target is not a military objective or the operation will breach the rule of proportionality.

The requirement to take precautions in attack has special resonance for both cyber attacks and the use of cyber assets during a kinetic attack. For instance, cyber means may be used to determine the nature of a cyber or kinetic target before it is attacked.[193] Such means may also be useful in estimating likely collateral damage and, following the attack, assessing whether reattack is needed. Even more importantly, cyber attacks may be less destructive or injurious than their kinetic counterparts,[194] as in the case of bringing down an integrated air defense system by cyber means rather than attacking associated radars and surface-to-air missile sites. Indeed, the availability of cyber capabilities may open new target sets, the attack on which may achieve desired effects with less risk of

---

[190] Tallinn Manual 2.0, *supra* note 3, r. 123, para. 2. *See also* UK Ministry of Defence, The Joint Service Manual of the Law of Armed Conflict, JSP 383, para. 5.17.2 (2004).

[191] Tallinn Manual 2.0, *supra* note 3, r. 124; Hague Regulations, *supra* note 123, art. 23(f); Additional Protocol I, *supra* note 122, art. 38(1); Additional Protocol II, *supra* note 117, art. 12; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem, art. 6(1), Dec. 8, 2005, 2404 U.N.T.S. 261. *See also* Customary IHL Study, *supra* note 141, rr. 58, 59, 61. Note that it is prohibited to use the UN emblem without United Nations approval. Tallinn Manual 2.0, *supra* note 3, r. 125; Additional Protocol I, *supra* note 122, art. 38(2); Customary IHL Study, *supra* note 143, r. 60.

[192] Tallinn Manual 2.0, *supra* note 3, ch. 17, sec. 7; Additional Protocol I, *supra* note 122, art. 57; Customary IHL Study, *supra* note 143, ch. 5.

[193] Tallinn Manual 2.0, *supra* note 3, r. 115; Additional Protocol I, *supra* note 122, art. 57(2)(a)(i); Customary IHL Study, *supra* note 143, r. 16. Prosecutor v. Stanislav Galić, Case No. IT-98-29-T, Trial Chamber judgment, ¶ 58 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003).

[194] Tallinn Manual 2.0, *supra* note 3, r. 116; Additional Protocol I, *supra* note 122, art. 57(2)(a)(ii); Customary IHL Study, *supra* note 143, r. 17.

collateral damage.[195] Consider a situation in which a commander wishes to disrupt the resupply of enemy forces by sea. One option would be to bomb the port facilities, an attack that may risk depriving the civilian population of food and other essentials arriving by sea and endanger those living near the port. However, instead of attacking the port facilities, cyber attacks that disrupt cyber infrastructure in a hardened facility that controls equipment used to offload military supplies could achieve the same effect while minimizing the impact on the civilian population.

Pursuant to the requirement to take precautions, an attacker must provide effective warning if civilians will be affected by an operation, "unless circumstances do not permit."[196] This requirement could include both warnings by cyber means of a kinetic attack, as in the case of text messages that urge the civilian population to take shelter in anticipation of an aerial attack, and warnings by cyber or other means of a cyber attack that poses danger for the general population. It must be emphasized that the requirement is subject to a condition of feasibility.[197] For instance, if warning of a cyber attack will alert the enemy in time to allow it to fashion an effective defense, the warning need not be issued.

G. *Proportionality*

The final step in the cyber targeting process is determining whether the cyber attack comports with the rule of proportionality. Pursuant to that rule, "a cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited."[198] Note that on its face the rule requires only the consideration of physical harm or injury; accordingly, mere inconvenience, irritation, stress or fear does not factor into a proportionality analysis.[199] Consider a denial of service attack against a military objective that interferes with civilian email services. The interference need not be considered when assessing whether damage caused by the attack is excessive relative to the attack's intended military gain. However, recall that in the context of the definition of an attack, deprivation of functionality qualifies as damage. In the same fashion, loss of the functionality of civilian cyber infrastructure is collateral damage for the purposes of the rule of proportionality.

---

[195] Tallinn Manual 2.0, *supra* note 3, r. 118; Additional Protocol I, *supra* note 122, art. 57(3); Customary IHL Study, *supra* note 143, r. 21.
[196] Tallinn Manual 2.0, *supra* note 3, r. 120; Hague Regulations, *supra* note 123, art. 26; Additional Protocol I, *supra* note 122, art. 57(2)(c); Customary IHL Study, *supra* note 143, r. 20.
[197] Tallinn Manual 2.0, *supra* note 3, r. 120, para. 8; Additional Protocols Commentary, *supra* note 146, para. 2223.
[198] Tallinn Manual 2.0, *supra* note 3, r. 113; Additional Protocol I, *supra* note 122, arts. 51(5)(b), 57(2)(iii). *See also* Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, art. 7, Mar. 26, 1999, 2253 U.N.T.S. 212; Amended Mines Protocol, *supra* note 182, art. 3(8); Mines Protocol, *supra* note 182, art. 3(3). *See also* Customary IHL Study, *supra* note 143, r. 14; Challenges Report, *supra* note 121, at 42–43.
[199] Tallinn Manual 2.0, *supra* note 3, r. 113, para. 5.

Both direct and indirect effects may qualify as collateral damage, an important consideration given the networked nature of cyber activities.[200] Thus, it is not only damage to civilian objects or injury to civilians caused by the initial effect of the cyber attack on the targeted cyber infrastructure that must be considered, but also any damage or injury to objects or persons that rely on such infrastructure or would otherwise be affected by damage to it. For instance, interference with a dual use communication system in a major metropolitan area could result in the disruption of emergency services. To the extent such disruption would foreseeably interfere with the treatment of injured persons, the likely harm to them would factor into the expected collateral damage assessment.

With respect to calculating the proportionality of a cyber attack, note that the collateral damage to be considered is that which was, or should have been, reasonably anticipated by those involved in the attack at the time they made their proportionality determination. The same is true with respect to the anticipated military advantage of an attack. In other words, compliance with the rule of proportionality is judged *ex ante*, not *post factum*.[201] The fact that a cyber attack results in collateral damage that is excessive relative to the eventual military advantage achieved does not render the attack unlawful so long as the attacker's judgment that it would not be excessive was reasonable in the circumstances. This caveat is especially significant with respect to cyber attacks because of the difficulty of surgically estimating likely collateral damage.

Finally, it must also be cautioned that IHL does not expressly define the term excessive. It has been suggested that extensive collateral damage is necessarily excessive.[202] A majority of the International Group of Experts concluded that this assertion misapprehends the law. On the one hand, if a cyber attack causes only slight damage or injury, but accrues little military advantage, it may violate the rule of proportionality. On the other, a cyber attack may cause significant damage or injury, but not violate the rule of proportionality because the military advantage resulting from the attack is great.

H. *Neutrality*

Cyber operations into or from neutral territory during an international armed conflict are subject to additional analysis due to applicability of the law neutrality.[203] To begin with, it has long been undisputed that belligerent states are

---

[200] Tallinn Manual 2.0, *supra* note 3, r. 113, para. 6. *See also* United States Submission to the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, *in* DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 2014, at 737; DoD Manual, *supra* note 10, para. 16.5.1.1.

[201] Tallinn Manual 2.0, *supra* note 3, r. 113, para. 11; Galić, *supra* note 193, ¶¶ 58–60; Trial of Wilhelm List and Others (The Hostages Trial), Case No. 47, VIII Law Reports of Trials of War Criminals 34, 69 (UN War Crimes Commission 1948) (the so-called "Rendulic Rule").

[202] Additional Protocols Commentary, *supra* note 146, para. 1980.

[203] Tallinn Manual 2.0, *supra* note 3, ch. 20; Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter

prohibited from exercising in neutral territory belligerent rights, which involve, *inter alia*, the conduct of military operations against the enemy.[204] Thus, if a belligerent engages in cyber operations related to the armed conflict from neutral territory, it has breached neutrality. Similarly, a belligerent may not conduct remote operations from outside the neutral state, as in the case of remotely taking control of neutral cyber infrastructure, whether government or private in nature, and use it to launch cyber attacks against its enemy.

In the cyber context, the pressing issue is when may a belligerent that has been targeted by cyber operations conducted from or through neutral territory respond by conducting its own cyber (or kinetic) operations into that territory. The International Group of Experts agreed that "if a neutral State fails to terminate the exercise of belligerent rights on its territory, the aggrieved party to the conflict may take such steps, including by cyber operations, as are necessary to counter that conduct."[205] Before an aggrieved belligerent may do so, the violation of neutrality by its adversary must have serious consequences and represent an immediate threat for that belligerent.[206] Mere inconvenience or irritation, even of a military nature, does not suffice. Effectively disrupting ongoing military operations or conducting cyber attacks would clearly cross the threshold.

The right of the neutral state to be free of belligerent cyber operations on its territory comes with a corresponding obligation to not knowingly allow them to occur.[207] The neutral state is entitled to take cyber measures to meet this obligation, but may not exceed those that are reasonably necessary to do so given the circumstances. If the neutral state is willing and able to act to put an end to the offending cyber operations, the aggrieved belligerent must defer to it in handling the situation.[208] Should the neutral state fail to comply with its obligation, the belligerent must warn, if feasible, the neutral to do so before acting. As a practical matter, this may not be possible because of the speed with which cyber operations can unfold.[209] If the neutral state is still unwilling or unable to address the situation, the belligerent may take those cyber or kinetic measures that are required to put an end to the offending cyber operations. In that the neutral state is protected by the law of neutrality and the principle of sovereignty, any belligerent operations must be strictly limited to those necessary to terminate its opponent's operations and comply fully with IHL rules.

Hague Convention V]; Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague Convention XIII].

[204] Tallinn Manual 2.0, *supra* note 3, r. 151; Hague Convention V, *supra* note 203, arts. 2, 3; Hague Convention XIII, *supra* note 203, arts. 2, 5.

[205] Tallinn Manual 2.0, *supra* note 3, r. 153. *See also* DoD Manual, *supra* note 10, para. 15.4.2.

[206] Tallinn Manual 2.0, *supra* note 3, r. 153, paras. 3 & 4. See analogously in the maritime warfare context, International Institute of Humanitarian Law, san Remo Manual on International Law Applicable to Armed Conflicts at Sea, r. 22 (Louise Doswald-Beck ed., 1995).

[207] Tallinn Manual 2.0, *supra* note 3, r. 152, Hague Convention V, *supra* note 203, art. 5.

[208] Tallinn Manual 2.0, *supra* note 3, r. 153, para. 4.

[209] *Id.*, r. 153, para. 5.

Conclusion

It is risky to set forth flowcharts and abstract analysis that might guide a state's cyber actions or its assessment of those conducted by other states and non-state actors. A particular cyber incident may have features that render it ill-fitted to analytical guidelines developed for paradigmatic clear-cut cases. Indeed, as was demonstrated in the Russian hacking of the U.S. election, actors in cyberspace will actively search for gray areas of international law within which to operate.

Therefore, this *vade mecum* must conclude with three cautionary notes. First, practitioners and academics have to be alert to the possibility that the cyber incident being analyzed does not fit neatly into this model. It is meant only to apply in a general sense. They should think of it as providing vector, not a precise route, through the legal morass that surrounds such incidents. Second, the analysis set forth is merely a skeleton of a highly complex body of law. Therefore, resorting to Tallinn Manual 2.0, upon which much of the discussion is based, is recommended since that work provides a highly granular treatment of the legal issues. Finally, it must be emphasized that our understanding of how international law applies to cyber operations is in its infancy; many issues lack clarity or are the subject of important disagreement, a point that important to bear in mind when deconstructing operations into their legal components. This caveat should be of special resonance for state legal advisors, for their advice will shape the legal policies that will in turn refine and develop the law governing cyberspace through state practice and expressions of *opinio juris*.[210]

[210] On the criticality of state practice and expressions of opinion juris regarding cyber operations, see Michael N. Schmitt and Sean Watts, *Beyond State Centrism: International Law and Non-State Actors in Cyberspace*, 21:3 J. CONFLICT & SECURITY L. 1 (2016).